TAMPEREEN TEKNILLINEN YLIOPISTO

IIKKA SALMELA

MITTAAMINEN OSANA LIIKETOIMINTALÄHTÖISTÄ TIETOTURVALLISUUDEN HALLINNOINTIA

Diplomityö

Tarkastaja: Professori Antti Lönnqvist
Tarkastaja ja aihe hyväksytty
teknis-taloudellisen tiedekuntaneuvoston
kokouksessa 5. joulukuuta 2012.

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietojohtamisen koulutusohjelma
SALMELA, IIKKA: Mittaaminen osana liiketoimintalähtöistä tietoturvallisuuden hallinnointia
Diplomityö, 105 sivua, 2 liitesivua
Joulukuu 2012
Pääaine: Tiedonhallinta
Tarkastaja: professori Antti Lönnqvist
Avainsanat: tietoturvallisuus, mittaaminen, tietoturvallisuuden hallinnointi, menestystekijät, tietoriski, mittaristoprojekti

Lähtökohtana tutkimukselle oli käytännön tarve tutkia, miten tietoturvallisuutta voidaan mitata sen hallinnoinnin näkökulmasta. Tutkimuksen tavoitteena oli kartoittaa, mitä tietoturvallisuuden tilaan liittyviä tietotarpeita yritysjohdolla ja tietoturvajohdolla on, jotta voidaan ymmärtää mitkä menestystekijät tietoturvallisuuteen vaikuttavat. Näiden menestystekijöiden kautta tavoitteena oli muodostaa liiketoimintalähtöinen mittaristo, joka tukee tietoturvallisuuden hallinnointia ja jonka avulla siitä voidaan viestiä johdolle.

Asetettua tavoitetta pyrittiin ensin ymmärtämään teoriaosassa, jossa käsiteanalyyttisen tutkimusotteen avulla muodostettiin viitekehys empiriaosalle. Viitekehys muodostettiin kirjallisuudesta löydetyn mittariston suunnitteluprosessin ja tasapainotetun tuloskortin perusteella, joita tarkasteltiin tietoturvallisuuden hallinnoinnin näkökulmasta. Empiriaosion lähtökohtana, oli selvittää miksi tutkimuksen kohdeyrityksen tietoturvallisuutta mitattaisiin ja mitkä ovat tärkeimmät tietotarpeet mittaamisen kannalta. Näihin kysymyksiin etsittiin vastausta teemahaastattelun avulla. Haastatteluun osallistu kohdeorganisaation edustajia johtoryhmästä, operatiivisesta johdosta ja tietoturvaorganisaatiosta. Haastatteluissa kerätty aineisto analysoitiin, minkä perusteella suunniteltiin mittaristo. Suunniteltua mittaristoa arvioitiin sekä kohdeyrityksen että kirjallisuuden näkökulmasta. Empiriaosiossa käytettiin tutkimusotteena toimintatutkimusta.

Tietoturvallisuuden holistisen tason mittaaminen on liiketoimintalähtöistä, joka perustuu esimerkiksi asiakkaiden vaatimuksiin tai muihin liiketoiminnan tietoturvallisuutta ohjaaviin vaatimuksiin. Nämä vaatimukset tulee huomioida osana sisäistä toimintaa ja ohjata toimintaa niiden mukaisesti. Kohdeyrityksen tietoturvallisuuden kannalta on tärkeää, että tietoturvallisuus huomioidaan tuotekehityksessä ja palveluita ylläpitävien prosessien osana. Ongelmaksi havaittiin, että kohdeyritys ei ole liiketoimintalähtöisesti asettanut tavoitetta tietoturvallisuudelle tai osoittanut sille kehitysvaatimuksia. Asiakasvaatimusten täyttämisen osoittaminen, laatu tuotekehityksessä ja sisäisessä tietoturvallisuudessa, toimialavertailu, palvelutason ylläpitäminen sekä tietoriskien esiintuominen osoittautuivat selkeiksi mittauksen kohteiksi.

Tutkimuksen tärkeimmät tulokset olivat tietoturvamittaristo, joka kuvailee kohdeyrityksen tietoturvallisuutta liiketoimintalähtöisesti, ja mittariston kehitysprojekti, jonka avulla voidaan muodostaa organisaation tietoturvallisuuden tilaa holistisella tasolla kuvaileva mittaristo. Mittariston avulla voidaan ymmärtää, mikä tietoturvallisuuden hallinnoinnin kannalta on liiketoiminnan näkökulmasta tärkeintä ja miten asetettuja tavoitteita saavutetaan.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information and Knowledge Management
SALMELA, IIKKA: Business Driven Information Security Measurement
Master of Science Thesis, 105 pages, 2 Appendix pages
December 2012
Major: Knowledge Management
Examiner: Professor Antti Lönnqvist
Keywords: information security, measurement, information security governance, key performance indicators, security risk, metrics project

The starting point for this research was a need for creating a holistic level security metrics from information security governance point of view. The goal of the research was to understand what management level needs to know about information security to support its governance. This was the way to understand the key performance indicators that affect the information security and create criteria for measuring information security based on indicators.

The research was divided into two parts: theoretical and empirical part. First, a conceptual research approach was used to understand the fundamentals of research topic and to create a theoretical framework for research. The framework consists of planning process for metrics system and a balanced scorecard. These were scrutinized from an information governance point of view. Then, an action science research approach was used to conduct the empirical part. First object in empirical part was to clarify why information security should be measured in the target company and what are the key performance indicators. Eight interviews were conducted to gain answers to these questions. The interview results were analyzed and a metric system was planned based on analysis. The metrics system was assessed both from literature and target company point of view.

Measuring the information security in holistic level must be business orientated and it must take customer needs or other parties' compliance needs into consideration at the internal operations. The target company wants to pay more attention to information security in its product development and conduct information security as a part of the processes that runs theirs services. A problem considering this is that the target company's management level haven't set goals for companywide information security nor pointed out what are the most important information security issues to develop. The most important information security performance indicators found in research were compliance to customer needs, quality in product development and internal security operations, benchmark score, service level, and ability to identify information security related risks.

There were two important results in the research. First result was a project for developing a holistic level security metrics system, which can be used to describe the state of information security. Second result was the metrics system itself, which supports the information security governance and reporting of information security. The target company should point out companywide information security goals and point out personnel's responsibility to support them in order to be able to measure their information security.

ALKUSANAT

Tämän tutkimuksen kirjoittamiseen on kulunut aikaa 698 tuntia, joiden aikana tutkijan suorituskykyä on pyritty nostamaan 51 litralla kahvia. Diplomityön kvalitatiivisen luonteen vuoksi lopputulosta ei näillä mittareilla voida arvioida, mutta muutamaa asiaa ne mielestäni kuvailevat erinomaisesti. Käytetyt tunnit osoittavat, että tutkimuksen aihe on mielenkiintoinen, johon on helposti voinut uppoutua ja jota tutkimusprosessin aikana olen oppinut ymmärtämään yllättävän paljon. Kahvin määrä taas kuvailee tutkimusprosessin suorittamista, joka on vaatinut täsmällisyyttä, päättäväisyyttä ja sitoutumista.

Vaikka diplomityön kirjoittaminen onkin henkilökohtainen suoritus, ei tutkimusprosessin toteuttaminen olisi onnistunut ilman tukea ja kannustusta. Työn ohjannut professori Antti Lönnqvist ansaitsee suuren kiitoksen, sillä hänen ammattitaidon, näkemyksen ja neuvojen ansiosta tutkimuksesta tuli monipuolinen ja osasin keskittyä oikeisiin asioihin. Kiitoksen ansaitsevat myös Nixu Oy, joka mahdollisti diplomityön tekemisen, ja työkaverit, jotka antoivat minulle arvokasta tukea ja palautetta koko tutkimuksen ajan. Erityisesti työn toinen ohjaaja, Jarkko Holappa, edesauttoi kokemuksellaan ja vankalla tietoturvaosaamisellaan työn etenemistä.

Diplomityö on koko opiskelu-urani huipentuma. Koko opiskelujeni ajan perheeni on tukenut, kannustanut ja inspiroinut minua uskomattoman paljon. Kiitos. Viimeiset ja rakkaimmat kiitokset haluan osoittaa avopuolisolleni ja tulevalle vaimolleni Annikalle, joka on kannustanut, motivoinut ja osoittanut täyden tukensa työn tekemiselle.

Tampereella 21.12.2012 Iikka Salmela

SISÄLLYS

1 JOHDANTO

1.1 Tutkimuksen tausta

Yritysten liiketoiminnassa tieto sen eri muodoissaan on muodostunut merkittäväksi menestykseen vaikuttavaksi tekijäksi. Tehokas tiedon käyttö on tärkeä kilpailutekijä, sillä usein tuote tai sen valmistaminen perustuu tietoon. Lisäksi perinteiset tuotantotekijät ovat melko helposti kaikkien saatavilla, jolloin yritysten erot muodostuvat sen mukaan, kuinka hyvin ja tehokkaasti tietoa pystytään hyödyntämään. Jotta tietoa voidaan hyödyntää, tulee sitä pystyä tallentamaan hyvin jäsennetysti, tiedonsiirron pitää olla nopeaa ja käytettävän tiedon tulee olla oikeellista. Yritysten tehokkaan toiminnan kannalta on myös varmistettava, että oikea tieto saavuttaa oikean henkilön oikeaan aikaan. Nämä tietoon liittyvät tavoitteet ovat lähtökohta tiedon saatavuuden, eheyden ja luottamuksellisuuden varmistamiselle, joka on tietoturvallisuuden hallinnoinnin päätehtävä (mm. Tipton & Krause 2004; Jaquith 2007; Brotby 2009; Whitman & Mattord 2011).

Yritysten omistama tieto on siis muuttunut liiketoimintakriittiseksi kilpailutekijäksi ja lähes kaikki yrityksen laitteet ovat riippuvaisia tietojärjestelmistä. Myös tietoturvauhat ovat arkipäiväistyneet. Tästä syystä johdon on huomioitava tietoturvallisuus ja varmistettava, että sen hallinnointia toteutetaan liiketoiminnan tarpeiden mukaisesti. Tietoturvallisuuden hallinnointi saa vaatimuksia liiketoiminnan lisäksi usein asiakkailta ja laeista, joiden mukaan organisaation tietoturvallisuus on vietävä käytäntöön (Baskerville & Dhillon 2008; Straub et al. 2008; Keyworth & Whitten 2010). Tietoturvallisuuden hallinnoinnin onnistumista on haastava arvioida liiketoimintalähtöisesti, sillä keinoja arvioida tietoturvallisuuden tilaa tai vertailla eri organisaatioiden tietoturvallisuutta ei ole (Jaquith 2007, Brotby 2009, Savola 2012). Perinteinen näkökulma yrityksen toiminnan arvioinnille muuttuvassa liiketoimintaympäristössä on mittaaminen. Esimerkiksi Kaplanin & Nortonin (1992) esittelemä tasapainotettu tuloskortti on tunnettu ja usein sovellettu mittariston viitekehys, jonka avulla liiketoimintaympäristöä mitataan ja tutkitaan. Mittaamisen avulla voidaan arvioida yrityksen menestystä, kykyä edetä strategian mukaisesti ja asettaa tavoitteita toiminnalle (mm. Otley 1999; van Decker 2010; Ylisirniö 2011).

Tietoturvallisuuden merkitys ja tietoturvavaatimukset liiketoiminnalle lisääntyvät jatkuvasti. Mittaaminen on puolestaan vakiintunut keino liiketoiminnan tulosten seuraamiseen. Näiden kahden asian yhdistäminen on mielenkiintoista useastakin näkökulmasta. Esimerkiksi Sun Tzun klassinen sitaatti, *”tunne itsesi ja tunne vihollinen, sadassakaan taistelussa et ole vaarassa”*, voidaan tulkita tietoturvallisuuden mittaamisen kautta. Tie-

toturvallisuutta mittaamalla pyritään ymmärtämään yrityksen oman tietoturvallisuuden tilaa ja vertaamaan sitä tietoturvallisuuteen liittyviin uhkiin ja vaatimuksiin. Mittaamisen avulla voidaan myös optimoida tietoturvallisuuteen käytettäviä resursseja ja kehittää tietoturvallisuutta ylläpitäviä prosesseja (Barabanov et al. 2011; Savola et al. 2012). Liiketoiminnan kannalta mittareiden avulla tietoturvallisuus voidaan yhdistää osaksi muita organisaation tavoitteita ja varmistaa, että tietoturvallisuus ymmärretään kokonaisuutena (Savola et al. 2012).

Sekä tietoturvallisuus että liiketoiminnan menestyksen mittaaminen ovat tutkimusalueina hyvällä maturiteettitasolla ja teoreettisia sovelluksia on viety käytäntöön. Molemmista aihepiireistä löytyy empiirisiä tutkimuksia ja kattavia perusteoksia. Tietoturvallisuuden mittaaminen on kuitenkin suhteellisen uusi tutkimusalue, jota on tutkittu teknispainotteisesti (Jaquith 2007) ja tietoturvapäällikön näkökulmasta (Brotby 2009), sekä jonkin verran yksityiskohtaisimmista näkökulmista. Esimerkiksi Oulun Yliopistossa tietoturvallisuuden mittaamista pohditaan tietojärjestelmien näkökulmasta (Savola 2012). Usein mittarit liitetään vaatimustenmukaisuuteen tai riskienhallintaan. Jansen (2009) tiivistää aihepiirin haasteeksi, että empiirisesti ei ole osoitettu mittareita, joista olisi hyötyä liiketoiminnalle. Savolan (2012) mukaan mittareita on tutkittu jo jonkin verran, mutta käytäntöön niitä ei ole pystytty viemään. Suoraan johtoryhmätasolle suunnattuja mittareita ei ole tunnistettu.

Tämä diplomityö on tehty osana ITEA2 Predykot hanketta, jossa on mukana 16 eurooppalaista tietoturva-asiantuntija organisaatiota. Predykot hankkeen laajuus on 160 henkilötyövuotta ja sen tavoitteena on muuttaa tietoturvallisuuden hallinnoinnin fokus operatiivisesta perusasioiden parantamisesta osaksi liiketoimintaprosessien kehittämistä. Työn toimeksiantaja on Nixu Oy, joka on Pohjoismaiden suurin tietoturvakonsultointiin erikoistunut asiantuntijayritys. Tutkimuksen kohdeyritys, suomalainen pörssiyritys, esitellään tarpeellisin osin luvussa 5.

1.2 Tutkimuksen tavoitteet ja tutkimusongelma

Lähtökohtana tälle tutkimukselle on mielenkiinto liiketoimintalähtöisen tietoturvallisuuden mittaamiselle, jota on kirjallisuudessa tutkittu hyvin vähän. Tiedon kasvanut merkitys yrityksille lisää todennäköisesti liiketoimintajohdon kiinnostusta siitä, mikä on tietoturvallisuuden tila ja mitkä tekijät siihen vaikuttavat. Tämä tuo haasteita tietoturvallisuuden johtamiselle, jonka yksi tehtävä on raportoida tietoturvallisuuden tilasta liiketoimintajohdolle. Tämän tutkimuksen tavoitteena on kartoittaa, mitä tietoturvallisuuden tilaan liittyviä tietotarpeita liiketoimintajohdolla ja tietoturvapäälliköllä on sekä tunnistaa parhaiten tietoturvallisuuden tilaa kuvaavia menestystekijöitä. Menestystekijöiden avulla pyritään muodostamaan mittaristo, jonka avulla tietoturvallisuudesta voidaan kommunikoida ja joka kuvailee yrityksen tietoturvallisuuden tilaa ja sen kehittymistä.

Tämän tavoitteen pohjalta muodostuu diplomityön päätutkimuskysymys, jonka kautta tietoturvallisuuden mittaamiseen liittyviä ongelmia pyritään käsittelemään: *Miten yrityksen tietoturvallisuutta voidaan mitata niin, että mittaamisen avulla ymmärretään tietoturvallisuuden tila ja voidaan hallinnoida sitä tietoturvastrategian mukaisesti?* Päätutkimuskysymys on luonteeltaan todella haastava ja laaja, joten vastausta siihen on perusteltua etsiä alatutkimuskysymyksillä. Vastausta etsitään seuraavien tutkimuskysymysten avulla:

- Mitä tietoturvallisuus tarkoittaa osana liiketoimintaa ja mitä haasteita sen mittaamisessa on?
- Miksi kohdeyrityksen tietoturvallisuutta mitattaisiin ja mitä tietotarpeita eri johtotasoilla on tietoturvallisuuden suhteen?
- Mitkä menestystekijät kuvailevat kohdeyrityksen tietoturvallisuuden tilaa parhaiten?
- Miten kohdeyrityksen tietoturvallisuutta voidaan mitata?

Tutkimuskysymyksiin pyritään löytämään vastauksia ensin teoriasta, jonka avulla muodostetaan peruskäsitys tutkimuksen aihepiiristä. Teoriaosuuden tavoitteena on muodostaa yleinen viitekehys, jonka perusteella mittaristo voidaan muodostaa. Tämän jälkeen syvennytään empiriaan, jonka avulla tutkimuskysymyksiin pyritään vastaamaan siten, että vastausten avulla voidaan suunnitella mittaristo ja perustella siihen liitettävät mittarit kohdeyrityksen liiketoiminnan näkökulmasta.

1.3 Tieteenkäsitys ja tutkimusote

Positivismi ja hermeneutiikka ovat tieteenkäsityksen kaksi valtakäsitystä. Positivismi on tieteellinen katsantotapa, joka hylkää kaikki epävarmat ja ei-havaittavissa olevat asiat. Se pohjautuu tosiasioihin ja realismiin, joka painottaa havaittavaa todellisuutta. Hermeneutiikka taas on katsantotapana päinvastainen, sillä se korostaa tulkintaa, asioiden merkitystä ja keskinäistä suhdetta sekä ymmärtämistä. Hermeneutiikassa painotetaan selitystaitoa ja käsitteiden tulkintaa. (Olkkonen 1994, s. 26-27.) Gummesson (2000, s. 5) kuvaa hermeneuttisen ja positivistisen tutkimuksen eron olevan siinä, että hermeneuttisessa tutkimuksessa pyritään ymmärtämään ja tulkitsemaan tutkittavaa asiaa kun taas positivistisessa tutkimuksessa kuvaillaan ja selitetään asioita. Katsantotapojen taustalla on kaksi erilaista filosofista koulukuntaa. Hermeneutiikka pohjautuu idealismiin ja positivismi realismiin. Näiden tiedon saamisen ja tunnistamisen peruskäsitysten pohjalta rakentuvat eri tieteenalojen vallitsevat käsitykset tieteen menetelmistä. Muodostuneita menetelmiä kutsutaan tutkimusotteiksi tai tutkimusstrategioiksi. (Olkkonen 1994, s. 28) Hermeneuttinen tutkimus liitetään usein kvalitatiiviseen, eli laadulliseen tutkimukseen, jossa tietoa tuotetaan tulkintojen, ilmiöiden välisten suhteiden ja niiden kehityksen kautta. Positivismi taas liitetään kvantitatiiviseen tutkimukseen, jossa kerätään määrämuotoista dataa ja tutustutaan siihen objektiivisesti. (Tuomi & Sarajärvi 2009.) Tässä tutki-

muksessa käytetään laadullisen tutkimuksen menetelmiä, sillä tutkimuksen kohteesta pyritään lisäämään ymmärrystä ja tulkintojen kautta muodostamaan kehitysehdotuksia.

Käsiteanalyyttinen tutkimusote on yksi liiketaloustieteessä käytetyistä tutkimusotteista (Neilimo & Näsi 1980, s. 50). Tutkimusotteeltaan se on vahvasti teoreettinen ja sen tavoitteena on kuvata, tunnistaa ja luokitella ilmiöitä (Neilimo & Näsi 1980, s. 50; Olkkonen 1994, s. 65). Liiketaloustieteen tutkimuksessa on tyypillistä, että empiirisen tutkimuksen ohella käytetään käsiteanalyyttista tutkimusotetta, jonka avulla luodaan viitekehys empiiriselle osiolle (Hannula et al. 2002, s. 8). Tämän tutkimuksen teoriaosan tutkimusote on käsiteanalyyttinen, sillä siinä pyritään kuvailemaan tietoturvallisuuden mittaamista, siihen liittyviä ilmiöitä ja luokitteluja kirjallisuuden avulla. Tutkimuksessa hyödynnetyn teorian pohjalta tavoitteena on esitellä viitekehys, jonka avulla tutkimuksen empiirinen osio voidaan suorittaa ja ymmärtää mahdollisimman hyvin. Teoreettista ymmärrystä voidaan soveltaa mittareiden kehittämiseen ja analysoida sen pohjalta empiirisessä osiossa löydettyjä tuloksia.

Teoriaosuuden havainnot antavat pohjan työn empiiriselle osiolle, jossa vastataan tutkimuskysymyksiin tutkimuksen kohdeyrityksen näkökulmasta. Yin (2003, s 5-7) esittää, että tutkimusotetta valittaessa tulisi kiinnittää huomio seuraaviin seikkoihin.

- Tutkimusongelman ja tutkimuskysymysten tyyppi
- Tutkijan kontrolli tutkimuksen kohteeseen ja sen käyttäytymiseen
- Tutkimuksen fokus menneen ja nykyhetken välillä

Näistä kysymyksistä tärkein on ensimmäinen, eli tutkimusongelman tyyppi. Tutkimuskysymykset voidaan jaotella sen mukaan, minkä tyyppiseen kysymykseen niiden avulla pyritään vastaamaan. Kysymystyyppejä ovat ”mitä?”, ”miten?”, ”miksi?” ja ”missä?”. ”Mitä?” kysymykset jaetaan kahteen tyyppiin: kuvaileviin ja mittaaviin. Kuvailevien ”mitä?”-kysymysten tavoitteena on luoda hypoteeseja ja ehdotuksia myöhempää tutkimusta varten. Mittaavat taas hakevat vastauksia ”kuinka paljon?” tai ”kuinka monta?” tyyppisiin kysymyksiin. (Yin 2003, s. 5-6.) Tässä tutkimuksessa pyritään kuvailevien ”mitä”-kysymysten avulla selvittämään mittauksen kohteita ja mittaustarpeita kohdeyrityksessä, jotta voidaan vastata päätutkimuskysymykseen, joka on ”miten?”-tyyppinen. Ghaurin & Gronhaugin (2005) mukaan tapaustutkimusta on perusteltua käyttää tutkimusotteena, kun tutkimuskysymys alkaa sanalla ”miten” tai ”miksi”.

Tutkijan kontrollilla tutkimuksen kohteeseen tarkoitetaan sitä, onko tutkijan tarkoitus vaikuttaa tutkimukseen liittyviin tekijöihin (Yin 2003, s. 7). Tässä tutkimuksessa on tavoitteena löytää kohdeyrityksestä sellaisia tekijöitä, joilla voidaan kuvailla yrityksen tietoturvallisuuden tilaa. Tutkimusaineisto kerätään vaikuttamatta kohdeyrityksen toimintaan ja sen perusteella pyritään muodostamaan kehitysehdotuksia. Kehitysehdotuksena muodostetaan kohdeyrityksen tietoturvaa kuvailevia mittareita ja niihin liittyviä toimintasuosituksia. Viimeiseen tutkimusotteeseen vaikuttavaan seikkaan Yin (2003, s.

8) kehottaa pohtimaan tutkimuksen ajallista fokusta. Tässä tutkimuksessa kohdeyrityksen tietoturvallisuuden tilaan vaikuttavia asioita pyritään selvittämään nykytilassaan.

Kolmen tutkimusotetta ohjaavan perusteella tutkimuksen empiirisen osuuden tutkimusotteeksi sopii parhaiten tapaustutkimus. Tapaustutkimus käsittelee usein organisaation toimintaa, johtamista tai kehitysprojekteja ja sen tuloksena voivat olla esimerkiksi muutokset kohdeorganisaatiossa tai niihin tähtäävät tavoitteet (Olkkonen 1994, s. 72-73.) Lisäksi tapaustutkimukselle on tyypillistä, että yksittäisestä tapauksesta tuotetaan syvällistä ja yksityiskohtaista tietoa sekä kuvaillaan tutkittavaa ilmiötä valitun kohteen näkökulmasta pyrkimättä luomaan yleistettäviä malleja (Saarela-Kinnunen & Eskola 2001, s. 159).

Tutkimusotteen valinta ohjaa tutkimuksessa käytettävän tutkimusmenetelmän valintaa. Tämän tutkimuksen pääasiallinen tutkimusmenetelmä on toimintatutkimus, jonka tukena ja aineistonkeruumenetelmänä käytetään teemahaastattelua. Toimintatutkimus on laadullisen tutkimuksen menetelmä, jossa tutkija pyrkii vaikuttamaan sekä kohdeyrityksen yrityksen toimintaan että tieteelliseen tutkimukseen. Se soveltuu tutkimukseen, jossa pyritään ymmärtämään, suunnittelemaan ja toteuttamaan muutosta liiketoiminnassa. (Gummesson 2000, s. 119-120.) Tapaustutkimuksen aineisto taas voi koostua sekä kvantitatiivisesta että kvalitatiivisesta aineistosta. (Yin 2003, s. 8, 15.) Tämän toimintatutkimuksen tueksi kerätään aineistoa teemahaastattelun avulla, joten tutkimus ja sen tulokset ovat kvalitatiivisia. Tutkimusmenetelmät esitellään tarkemmalla tasolla luvussa viisi.

1.4 Tutkimuksen rajaaminen ja rakenne

Tutkimuksessa käsitellään kahta teemaa: tietoturvallisuutta ja mittaamista. Näitä teemat pyritään tarkastelemaan organisaation johtamisen näkökulmasta. Organisaation johtamista ei tutkimuksessa kuitenkaan esitellä yleisjohtamisen näkökulmasta, vaan tietoturvallisuuden hallinnoinnin ja mittaamisen ohella. Tietoturvallisuus on perusteltua käydä omana aihepiirinään läpi, jotta mittaamisen kohde ymmärretään. Ennen kuin mitään voidaan mitata, tulee se pystyä kuvailemaan (Kaplan & Norton 2004). Mittaamisen teorian ymmärtäminen antaa valmiudet suunnitella mittareita ja ymmärtää paremmin syitä sille, miksi mitataan. Työssä teemoja pyritään tarkastelemaan johdon ja tietoturvapäällikön näkökulmasta yrityksen liiketoiminnan ja hallinnollisen tietoturvallisuuden viitekehyksessä. Kuvassa 1.2 on havainnollistettu tutkimuksen teemoja. Kuvan keskellä esitetään tutkimuksen fokus.

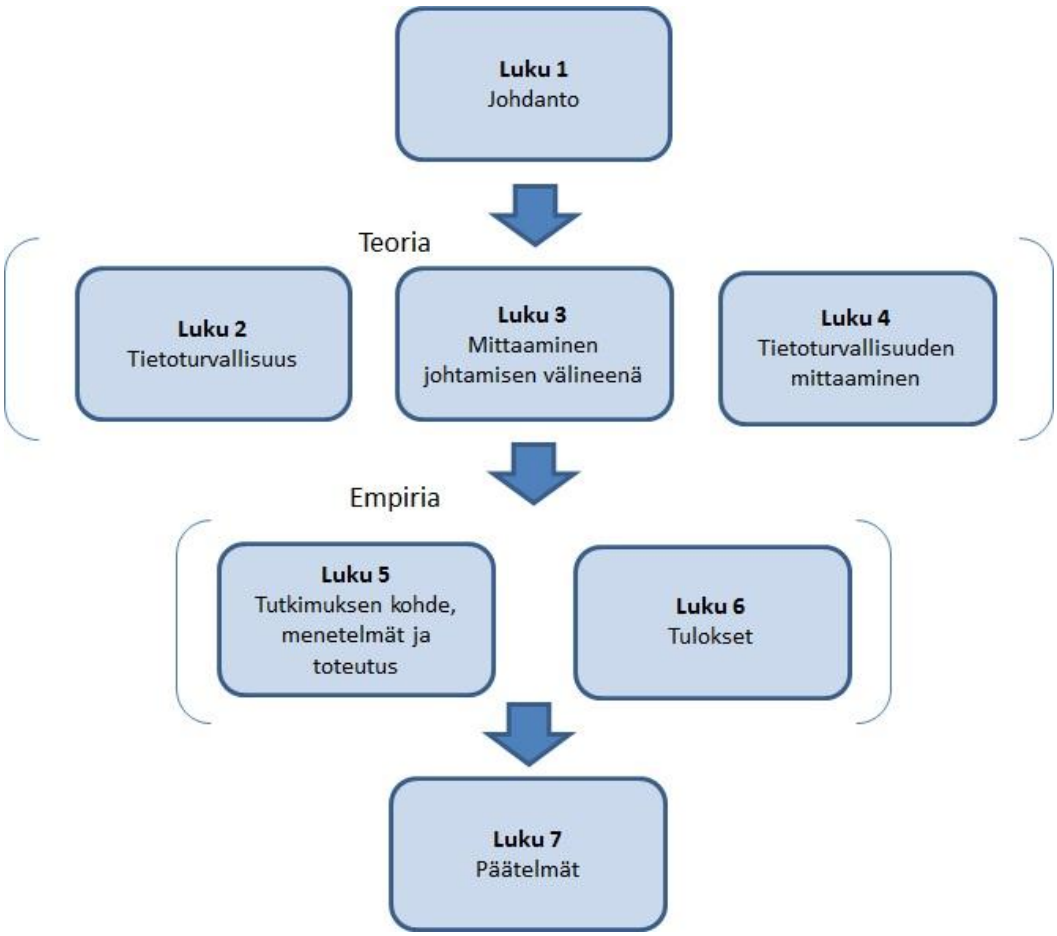
Kuva 1.2. *Tutkimuksen teemat.*

Kairab (2005, s. 46) kuvailee tietoturvallisuuden organisaation toiminnaksi, jossa toteutetaan yrityksen tietoturvastrategiaa eri toimintojen, esimerkiksi koulutuksen, toimeenpanon ja työkalujen, näkökulmista. Tässä tutkimuksessa käsitellään tietoturvallisuuden mittaamista ja keskitytään tarkastelemaan tietoturvallisuutta hallinnoinnin näkökulmasta ja kohdeyrityksen liiketoimintajohdon tietotarpeita sen osalta. Näiden perusteella tutkitaan, kuinka mittareita voidaan hyödyntää tietoturvastrategian ja siitä jalkautuvien toimintojen toteuttamisessa. Tietoturvatoimintojen suhdetta toisiinsa ei tutkita, vaan niistä pyritään löytämään menestystekijöitä ja tavoitteiden saavuttamista kuvaavia indikaattoreita. Tutkimuksessa perehdytään yleisesti tunnetuista tietoturvallisuuden osa-alueista erityisesti hallinnollisen tietoturvallisuuden mittaamiseen ja siihen, kuinka muiden osa-alueiden tilaa voidaan kuvata yksinkertaisilla mittareilla. Muut tunnetut osa-alueet esitellään lyhyesti luvussa 2.

Liiketoiminnan jatkuvuudenhallinta voidaan nähdä yhtenä tietoturvallisuuden osa-alueena (Tipton & Krause 2004, s.1642; Whitman & Mattord 2011, s.232; ISO/IEC 27001:fi). Jatkuvuudenhallintaa ei tämän tutkimuksen puitteissa käsitellä sen laajuuden vuoksi, vaan todetaan, että tietoturvallisuuden toimivuudella on suuri merkitys liiketoiminnan jatkuvuudelle. Mittareiden avulla voitaneen myös arvioida tietoturvallisuuden jatkuvuussuunnitelmaa, mutta näihin ei oteta tämän tutkimuksen puitteissa kantaa. ISO/IEC 27001:fi käsittelee turvallista tietojärjestelmien hankintaa, kehitystä ja ylläpitoa, sekä ohjeistaa tietoturvahäiriöiden hallinnasta. Näitä asioita ei työssä käsitellä, vaan näiden kehittäminen oletetaan olevan osa korkeamman tason tietoturvallisuuden kehittämistä.

Mittaamisen näkökulmasta tietoturvallisuuden eri osa-alueilta pyritään löytämään toimintoja, joita voidaan mittaamisen avulla analysoida, ohjata ja johtaa. Mittaamisen teoriaa käsitellään mittariston suunnittelun, tasapainotetun mittariston ja organisaation suorituskyvyn mittaamisen näkökulmasta. Tietoturvan mittaaminen voidaan jaotella esimerkiksi teknisiin, operationaalisiin ja johtamisen mittareihin (Henning 2001; Vaughn et. al. 2003). Tämän tutkimuksen laajuudessa ei käsitellä teknisiä ja operationaalisia mittareita, vaan pyritään muodostamaan liiketoimintalähtöinen mittaristo tietoturvallisuuden hallinnoinnin tueksi. Muun muassa Jaquith (2007) ja Brotby (2009) esittelevät jonkin verran tietoturvakustannuksiin liittyviä mittareita, jotka usein liitettään hallinnointia tukeviksi mittareiksi. Tietoturvallisuuden kustannuksia voisi tutkia pikemminkin laadun kustannusten kautta, joten ne rajataan tämän tutkimuksen ulkopuolelle.

Tutkimus koostuu seitsemästä eri elementistä. Kuvassa 1.3 esitellään nämä elementit, joiden mukaan tutkimus etenee. Luvut kaksi, kolme ja neljä käsittelevät aihepiirin teoriaa ja luvut viisi ja kuusi toteutetaan tapaustutkimuksena.



Kuva 1.3. *Tutkimuksen rakenne.*

Tietoturvallisuuteen liittyvät käsitteet ja erityispiirteet esitellään luvussa kaksi. Tietoturvallisuutta esitellään aluksi perinteisestä osa-alueiden ja ulottuvuuksien näkökulmasta,

jonka jälkeen tutkitaan mitä tietoturvallisuus on osana organisaation toimintaa. Organisaation toiminnasta päädytään pohtimaan tietoturvastrategiaa ja sitä, miten sen kautta voidaan muodostaa tietoturvapolitiikka ja tietoturvallisuuden hallinnointi. Lisäksi käsitellään syitä kehittää tietoturvallisuutta.

Tutkimuksen kolmannessa luvussa pohditaan mitä organisaation suorituskyky tarkoittaa ja miten sitä voidaan mitata osana johtamista. Tämän lisäksi esitellään tasapainotettu tuloskortti ja pyritään hahmottamaan, miten tietoturvallisuutta esitellään sen osana. Luvun lopuksi tutkitaan, miten mittariston suunnitteluprosessi etenee ja mitä sen osana tulee huomioida.

Tietoturvallisuuden mittaamista käsittelevässä luvussa neljä esitellään käsitteitä ja luokitteluja, jotka liittyvät tietoturvallisuuden mittaamiseen. Tämän lisäksi esitellään haasteita ja perustellaan, miksi tietoturvallisuutta pitäisi mitata. Lopuksi esitellään hyvän tietoturvamittarin ominaisuuksia ja viitekehys mittausprosessille.

Luku viisi esittelee tutkimuksen empiirisessä osuudessa käytettävän tutkimusotteen ja tutkimusmenetelmät, jotka muodostavat mittaristoprojektin. Tutkimusmenetelmiin liittyen esitellään myös haastatteluissa kerätyn aineiston analyysimenetelmä. Taustatietona tuloksille kuvaillaan kohdeyritystä ja esitellään haastatellut henkilöt tutkimukselle relevantein osin.

Tutkimuksessa saavutetut tulokset kuvaillaan luvussa kuusi. Tulokset käydään läpi teemoittain ja tuloksia analysoidessa löydettyjen ylä- ja alaluokkien kautta. Tulosten esittelyssä on yhteys luvussa kolme esiteltyyn tasapainotettuun tuloskorttiin.

Luvussa seitsemän esitetään tutkimuksen teoreettiset ja käytännön päätelmät, joiden perusteella annetaan suosituksia kohdeyritykselle. Luku seitsemän kattaa myös tutkimuksen tarkastelun ja sen onnistumisen analysoinnin tutkijan näkökulmasta. Lisäksi siinä pohditaan aihepiiriin liittyviä jatkotutkimusaiheita.

2 TIETOTURVALLISUUS

Tässä luvussa määritellään osa-alueet, joita tietoturvallisuudessa tulee huomioida ja esitellään tietoturvastrategian erityispiirteitä. Tietoturvallisuus ja sen hallinnointi on käsiteltävä kokonaisuutena, jotta pystytään ymmärtämään asioita, jotka ovat mittaamisen näkökulmasta tärkeitä. Tietoturvallisuuteen liittyvät toimintamallit, osa-alueet ja tiedon ulottuvuudet ovat keskeinen lähtökohta tutkittaessa tietoturvallisuuden mittaamista. Luvussa pohditaan myös tietoturvallisuuden suhtautumista liiketoimintajohtamiseen, riskienhallintaan ja tietojohtamiseen, jotta ymmärretään miten tietoturvallisuus suhtautuu liiketoimintaan.

2.1 Tieto ja turvallisuus

Tietoturvallisuus terminä koostuu kahdesta osasta: tiedosta ja turvallisuudesta. Näiden yhdistelmä koetaan usein teknisenä asiana, mutta molemmat termit käsittelevät huomattavasti laajempaa ilmiötä kuin pelkästään niiden teknistä tai fyysistä ulottuvuutta. Tieto jaetaan perinteisesti kolmeen eri tasoon: dataan, informaatioon ja tietämykseen. (Davenport & Prusak 1998, s. 2-6; Awad & Ghaziri 2004, s. 36-37). Lisäksi tieto voidaan nähdä älykkyytenä tai viisautena (Sydänmaanlakka 2004, s. 192). Datalla tarkoitetaan irrallista tietoa, joka koostuu numeroista, tekstistä, kuvista tai näiden yhdistelmistä. Data ei itsessään sisällä merkityksiä tai suhteita, eikä sitä ole välttämättä lajiteltu millään tavoin. Data muuttuu informaatioksi, kun sitä jäsennetään tai siihen liitetään selkeä asiayhteys. (Davenport & Prusak 1998, s. 2; Sydänmaanlakka 2004, s. 192-193)

Organisaatiossa dataa käsitellään tietotekniikan avulla. Tämä voi olla yksi syy sille, että tietoturvallisuus käsitetään teknisenä tietoa suojaavana elementtinä. Inhimillinen tekijä tulee kuvioon kuitenkin jo datan muuttuessa informaatioksi. Tällöin dataa jaotellaan asiayhteyteen sopiviksi taulukoiksi, joille annetaan otsikot. Voidaan nähdä, että data on informaatiota siinä vaiheessa, kun se pystytään viestimään ymmärrettävästi eteenpäin. Informaatio ei tässä vaiheessa vielä sitoudu henkilöön, vaan se on samanlaista kaikille sen käyttäjille. (Davenport & Prusak 1998, s. 3-4.) Thieraufin (2001, s. 9) mukaan informaatio muuttuu tietämykseksi, kun se sitoutuu henkilöön. Tietämys on ihmisten kokemusta, arvoja ja asiantuntijuutta, joiden avulla henkilö pystyy luomaan uusia asiayhteyksiä ja informaatiota (Davenport & Prusak 1998, s. 5). Tietoa voi siis tarkastella monesta näkökulmasta. Brotby (2011, s. 7) mainitsee tietoturvallisuuden kattavan puhutun, kirjoitetun, tulostetun ja elektronisen tiedon. Desouza (2007) lisää tietoturvallisuuteen liittyviksi asioiksi vielä tietämysturvallisuuden ja muun henkilökuntaan liittyvän turvallisuuden, jolla on tarkoitus suojata henkilöstön tietoja ja osaamista. Tässä työssä sana

tieto viittaa kaikkiin sen ulottuvuuksiin ja eri ulottuvuuksista keskusteltaessa puhutaan edellä esiteltyjen määritelmien mukaisesti.

Turvallisuudella tarkoitetaan usein resurssien suojaamista luvattomalta käytöltä. On kuitenkin huomioitava, että siihen liittyy myös resurssien suojaaminen siten, että uutta tietoa voidaan luoda ja että tieto ei tuhoudu. Turvallisuusuhka voi olla esimerkiksi vihamielinen hyökkäys, vahinko tai luonnonmullistus, joihin organisaation pitää varautua. (Straub et al. 2009.) Lisäksi turvallisuus nähdään organisaation eri osissa eri tavoin. Talousjohtajalle turvallisuusriskejä ovat kaikki, mikä aiheuttaa taloudellista epävarmuutta ja turhia kuluja. Ylimmälle johdolle turvallisuus voi tarkoittaa suojautumista kaikilta haitallisilta tapahtumilta, jotka vaikuttavat osakkeen arvoon tai yrityksen maineeseen. Myyntijohtaja taas näkee turvallisuuden tasaisessa myynnissä. Turvallisuus on jokaisen henkilökohtainen näkemys siitä, mikä on jonkin tapahtuman toivottu lopputulos ilman haittavaikutuksia tai esteitä tapahtuman kulkuun. Turvallisuuden ylläpitäminen on suojautumista epäsuotuisilta ja haitallisilta lopputuloksilta. (Brotby 2009) Tietoturvatapahtumalla viitataan tässä tutkimuksessa tietoturvallisuuteen liittyviin tapahtumiin, joilla on tai saattaa olla epäsuotuisa tai haitallinen lopputulos.

Tietoturvallisuus tarkoittaa käytännössä järjestelyjä, joilla pyritään varmistamaan ja säilyttämään tiedon eheys, käytettävyys ja luottamuksellisuus organisaatiossa (ISO/IEC 17799:2005). Tietoturvallisuuteen liittyvät järjestelyt tarkoittavat tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista siten, että niihin kohdistuvia riskejä voidaan hallita sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä (VAHTI 3/2007). Tietoturvallisuus on riskienhallintaa ja se on yksi yritysturvallisuuteen liittyvistä kokonaisuuksista. Tietoturvallisuus ymmärretään perinteisesti teknisestä näkökulmasta, joka vastaa tietoturvallisuuden alakäsitettä tietotekniikan turvallisuus. Tietotekniikan turvallisuus käsittää organisaation tietoliikenteeseen, laitteistoihin ja ohjelmistoihin liittyvän tietoturvallisuuden. (VAHTI 8/2008.) Tietoturvallisuus on käsite, joka sisältää teknologian lisäksi tietoturvallisuuspolitiikat, toimintaohjeet, tarkastukset ja jatkuvan oman toiminnan arvioinnin (Kairab 2005, s. 2-3).

Peltier et al. (2004, s. 1) tiivistävät tietoturvallisuuden tarkoittavan organisaatiolle arvokkaiden tietojen, ohjelmistojen ja laitteistojen turvaamista ja suojaamista. Peltierin tiivistystä tulkittaessa on huomioitava tiedon eri tasot, jolloin saadaan kokonaisvaltaisempi kuva siitä mitä tietoturvallisuus on. Koko organisaation toiminnan näkökulmasta tietoturvallisuus tarkoittaa Whitmanin & Mattordin (2011, s. 41-42) mukaan neljän toiminnon suorittamista:

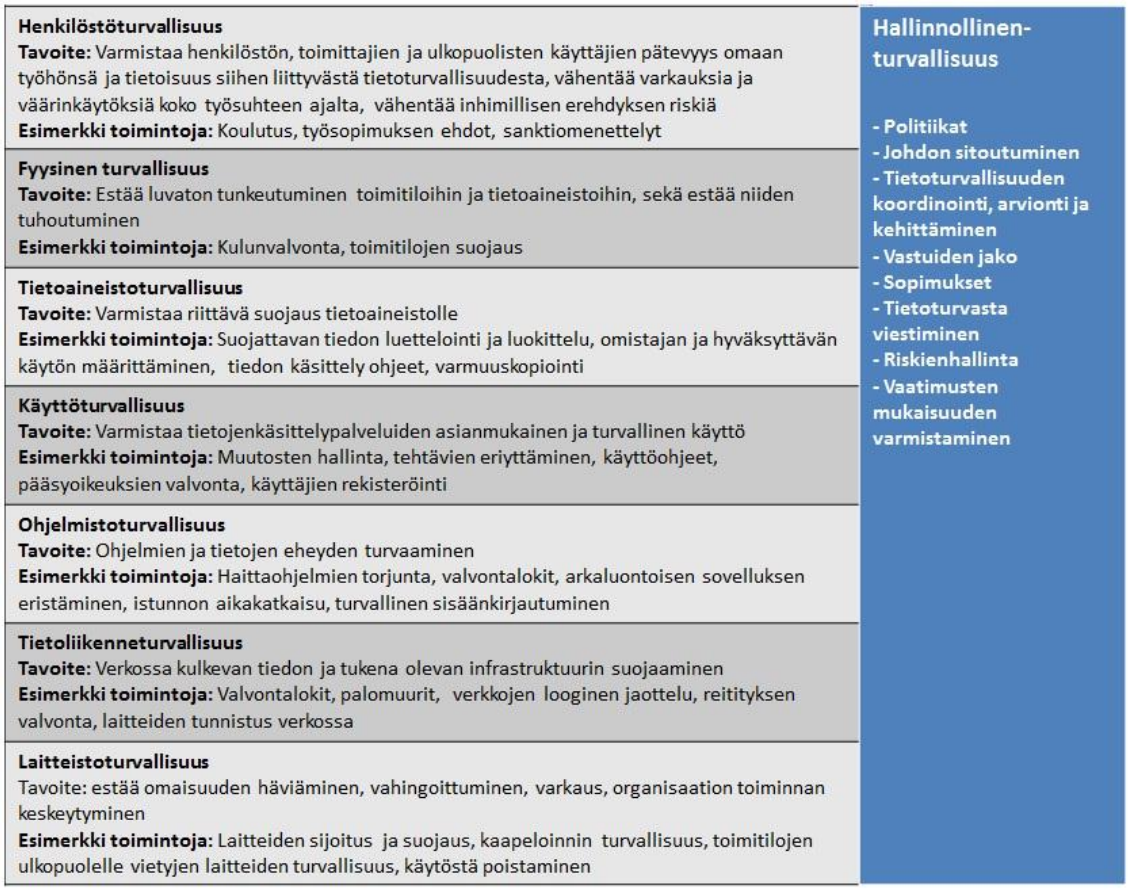
- Varmista organisaation toimintakyky
- Mahdollista sovellusten turvallinen käyttö
- Turvaa organisaation keräämät ja käyttämät tiedot
- Suojele teknisiä resursseja

Whitmanin & Mattordin (2011) esittelemät toiminnot kuvaavat tietoturvallisuuden laajuutta, sillä ne kattavat kaiken organisaation toiminnan. Ne huomioivat tekniset resurssit, niiden käytön ja niiden sisältämän tiedon. Tämä määritelmä jättää tietoturvallisuudesta edelleen teknisen kuvan, sillä inhimilliset toimet eivät suoranaisesti tule esiin määritelmästä. Esimerkiksi Dhillonin & Backhousen (2000) mukaan tietoturvallisuus kattaa myös ihmisten rehellisyyden, etiikan sekä ihmisten tietämyksen saatavilla olon ja eheyden. Kairab (2005, s. 9) mainitsee tätä tukien, että tietoturvallisuudessa tulee huomioida ihmisten toiminnan, prosessien sekä teknologian näkökulma. Näiden painotukset tietoturvatoiminnassa menevät Kyrölän (2001) mukaan siten, että kahdeksankymmentä prosenttia toiminnasta on esimiesten ja työntekijöiden toimintoja, päätöksentekoa ja muita inhimillisiä asioita ja kaksikymmentä prosenttia teknologisia ratkaisuja.

Päätutkimuskysymyksessä ja tutkimuksessa yleisesti käytetty ilmaus ”tietoturvallisuuden tila” voidaan edellä kuvailtujen käsitteiden perusteella nähdä tarkoittavan sellaista tietoturvallisuuden toteuttamista, jossa ihmisten toiminta, teknologia ja prosessit on huomioitu riittävän hyvin hallinnollisesta ja teknisestä näkökulmasta. Tietoturvallisuuden tilan kehittäminen ja hyvän tason ylläpitäminen auttaa suojautumaan organisaation tietoon kohdistuvilta tapahtumilta, jotka ovat organisaatiolle epäsuotuisia ja haitallisia. Tietoturvallisuutta mittaamalla organisaatio voi osoittaa, että sen tietoturvallisuuden tila on tavoitteen mukainen tai kehittää sitä kohti asetettuja tavoitteita (Jansen 2009). Tietoturvallisuuden tilaa voidaan pohtia tietoturvallisuuden osa-alueiden kautta, mutta ne tulee ymmärtää osana organisaation toimintaa ja tietoturvallisuuden hallinnointia kokonaisuudessaan.

2.2 Tietoturvallisuuden osa-alueet ja ulottuvuudet

Tietoturvallisuus jaetaan osa-alueisiin sekä organisaation toiminnan näkökulmasta että tiedon arvoa tuovien ominaisuuksien näkökulmasta (mm. Tipton & Krause 2004, Whitman & Mattord 2011). Tapoja jaotella tietoturvallisuutta on useita aihealueen monipuolisuuden ja kompleksisuuden vuoksi. Perinteinen jaottelutapa on standardin ISO/IEC 27001 mukainen jaottelu, jota muun muassa Tipton & Krause (2004) ja Whitman & Mattord (2011) käyttävät esitellessään aihepiiriä. Samankaltaista jaottelua käyttää valtionhallinto julkaisemassaan osa-aluejaossa ja ohjeistuksissaan. Kuvassa 2.1 esitellään yleisesti tunnettu kahdeksan osa-alueen jaottelu. Kuvassa esitellään lyhyesti tavoite, johon eri osa-alueiden toteuttamisella pyritään. Lisäksi annetaan esimerkkejä tietoturvatoiminnoista. Tietoturvatoiminnoilla tarkoitetaan tässä tutkimuksessa keinoja, joiden avulla organisaation tietoturvallisuutta pidetään käytännössä yllä, eli estetään epäsuotuisten ja haitallisia tapahtumia organisaation tietoon liittyen.



Kuva 2.1. *Tietoturvallisuuden osa-alueet. (Mukailtu lähteistä ISO/IEC 27001 & VAHTI)*

Tietoturvallisuuden osa-alueet jaetaan kolmeen perusulottuvuuteen, joiden avulla tietoturvallisuus perinteisesti myös määritellään. Nämä ovat eheys, luottamuksellisuus ja saatavuus (mm. Tipton & Krause 2004; Whitman & Mattord 2011; ISO/IEC 27001:fi). Eheydellä tarkoitetaan tietojen tai järjestelmien sisäistä ristiriidattomuutta, ajantasaisuutta, oikeellisuutta ja käyttökelpoisuutta. Eheys on ominaisuus, jonka perusteella voidaan ilmentää, että tietoa ei ole valtuudettomasti muutettu. Luottamuksellisuudella viitataan siihen, että tieto säilyy luottamuksellisena ja siihen, että oikeudet tiedon käyttöön jaetaan oikein. Saatavuus voidaan ymmärtää tiedon käytettävyytenä, joka tarkoittaa että tieto on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. (VAHTI 8/2008.)

Whitman & Mattord (2011, s. 13) kuvailevat, että luottamuksellisuus liittyy usein yksityisyyden suojaan, joka on erityisen tärkeää silloin kun se liittyy henkilökohtaiseen tietoon. Toinen esimerkki luottamuksellisesta tiedosta on liiketoimintatieto. Keinoja, joilla luottamuksellisuutta pyritään lisäämään, on tietojen luokittelu, turvallinen dokumenttien säilytys, työntekijöiden kouluttaminen ja turvalliset menettelytavat tietoa käsitellessä. Jotta tietoa voidaan ymmärtää, tulee sen olla eheää. Eheys on tietojärjestelmiin tallennettavan ja tiedon siirron kannalta merkittävää, siellä tieto menettää arvonsa, mikäli se ei ole käyttötarkoitukseen soveltuvassa muodossa. Tiedon eheys varmistetaan esimer-

kiksi erilaisilla tarkistusarvoilla tai tiivisteillä, joiden kautta nähdään onko tietoaineisto säilynyt muuttumattomana. Tieto menettää arvonsa, mikäli se ei ole saatavilla silloin, kun henkilö tai tietojärjestelmä tarvitsee sitä. (Whitman & Mattord 2011, s. 12-14.) Saatavuuden ja luottamuksellisuuden välillä on yhteys. Mikäli luottamuksellisuus määritetään todella suureksi, tulee tieto tallentaa siten, että ulkopuolisten on huomattavan vaikea päästä siihen käsiksi. Tällöin saatavuus heikkenee, sillä tieto on salattu huolellisesti ja on siten vaikeasti saatavilla. On myös huomioitava, että tietoa ei välttämättä kannata edes tallentaa, mikäli se ei ole eheää.

Muita kirjallisuudesta löytyviä ulottuvuuksia tietoturvallisuudelle ovat tarkastettavuus, kiistämättömyys, täsmällisyys, autenttisuus, hyödyllisyys ja hallussapito (Brotby 2009; Whitman & Mattord 2011). Näistä mielenkiintoisimpia ovat kiistämättömyys ja tarkastettavuus, jotka viittaavat tiedon käyttöön. Muut termit voidaan nähdä perinteisen kolmijaon yhdistelminä. Valtionhallinto määrittelee kiistämättömyyden tarkoittavan menetelmiä, joiden avulla osoitetaan että tietty henkilö on lähettänyt tai vastaanottanut viestin tai että jokin tapahtuma on jätetty käsiteltäväksi. Tarkastettavuus taas tarkoittaa järjestelmän ominaisuuksia, joiden avulla tuodaan esille sen toiminnassa esiintyviä virheitä, epäsäännöllisyyksiä ja väärinkäytöksiä. (VAHTI 8/2008.) Nämä ominaisuudet kuvastavat kontrollikeinoja, joilla tiedon käyttöä pystytään valvomaan. Toisin sanoen niiden avulla varmistetaan, että tietoturvallisuuden tila on tyydyttävä ja löydetään poikkeamia toiminnassa. Kiistämättömyys ja tarkastettavuus voidaan liittää olennaiseksi osaksi tiedon omistajuutta, jolloin tiedon käsittely on jonkun vastuulla ja sen käyttöä valvotaan.

Tietoturvallisuuden ongelmana on usein se, että se ei ole sisäänrakennettuna osana organisaation muuta toimintaa, vaan siihen liittyviä toimintoja pyritään toteuttamaan erillisinä komponentteina, jotka usein heikentävät käytettävyyttä. Kayworth & Whitten (2010) kritisoivat sitä, että tietoturvallisuutta pidetään teknisenä asiana, jonka johdosta sitä toteutetaan usein tietotekniikkayksikön alaisuudessa. Tietoturvallisuus voidaan esimerkiksi liittää kiinteäksi osaksi yritysturvallisuuden, riskienhallinnan ja henkilöstöhallinnan toimintaan, sekä liiketoimintaprosessien osaksi tarkastuslistojen, kontrollien ja standarditoimintatapojen avulla. Esimerkiksi automaattinen varmuuskopiointi, kertakirjautuminen järjestelmiin ja keskitetty virustorjunta ovat liiketoimintaa tehostavia keinoja, jotka vähentävät työntekijöiden tarvetta huolehtia tietoturvallisuudesta ja tehostavat siten työntekoa. Yksi tietoturvamittari voisikin olla, kuinka suuri osa tunnetuista tehokkuutta lisäävistä tietoturvatoiminnoista on otettu käyttöön.

2.3 Tietoturvallisuus osana organisaation toimintaa

2.3.1 Tietoturvallisuus osana johtamista

Tieto on organisaation kriittinen kilpailutekijä, sillä sen toiminta voi lamaantua täysin mikäli keskeiset toimintaympäristön tarvitsemat tiedot, tietojärjestelmät ja yhteydet ei-

vät toimi suunnitellusti tai ole saatavilla. Lisäksi päätökset, jotka perustuvat epäeheään tietoon voivat aiheuttaa vakavia vahinkoja organisaation toiminnalle ja imagolle. (Vahti 2/2011.) Tietoturvallisuus on tukitoiminto, jolla suojellaan organisaation tietoja. Johtoryhmätasolla tärkein tehtävä on varmistaa, että tietoturvallisuus on järjestetty siten, että se tukee organisaation tavoitteiden toteutumista. Tähän kuuluu tietoriskien yhdistäminen muuhun riskienhallintaan, tietoturvainvestointien optimoiminen ja tietoturvallisuuden toteutumisen varmistaminen. Lisäksi johdon on huolehdittava siitä, että yrityksen resursseja käytetään tehokkaasti tietoturvatavoitteiden saavuttamiseksi. (Brotby 2008, s. 83-84.) Yksityiskohtaisempia tietoturvallisuuteen liittyviä asioita, joita johdon on huomioitava, ovat toiminnan lainmukaisuus, raportointi sekä poikkeamien ja erityistilanteiden hallinta (Vahti 2/2011). Näihin asioihin johtoryhmä voi ottaa kantaa tietoturvapolitiikan kautta, jossa se antaa tukensa tietoturvatoiminnalle ja osoittaa tietoturvallisuuden tärkeyden liiketoiminnan jatkuvuudelle (Krutz & Vines 2004, s. 20). Tietoturvapolitiikkaan liittyvät asiat, jotka johtoryhmän tulee sen yhteydessä huomioida, esitellään luvussa 2.4.

Vaikka johtoryhmän tulee varmistaa, että tietoturvallisuuden organisointi ja sen johtaminen ovat yrityksessä kunnossa, voi se antaa vastuun näiden käytäntöön viemisestä esimerkiksi toiselle organisaation osalle. Usein yrityksissä onkin tietoturvapäällikkö, joka raportoi johdolle tietoturvallisuuden tilasta, kehityksestä ja tietoturvavelvoitteiden toteutumisesta. (Vahti 2/2011.) Tietoturvapäällikön lisäksi eri yksiköillä tai liiketoiminta-alueilla voi olla tietoturvallisuuden vastuuhenkilö, joka omistaa tiedon ja määrittelee tiedon käyttötavat, sekä tietoturva-asiantuntija, joka vastaa tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Tietoturvallisuuden vastuuhenkilö on käytännössä liiketoimintayksikön johtaja tai järjestelmänomistaja, joka sitten valtuuttaa päivittäisen tietoturvallisuudesta huolehtimisen tietoturva-asiantuntijalle. Tietoturva-asiantuntija voi käytännössä olla järjestelmäasiantuntija, joka huolehtii järjestelmän tietoturvallisuudesta yrityksen määrittelemien periaatteiden mukaan. Yrityksen muut työntekijät ovat tiedon käyttäjiä, joilla on vastuu siitä, miten he käyttävät tietoa ja velvollisuus käyttää sitä yrityksen määrittelemällä tavalla. (Krutz & Vines 2004, s. 15-16, 23)

Pääasialliset sidosryhmät osana tietoturvallisuuden johtamista ovat tietohallintojohtaja, liiketoimintajohtajat ja lopulta kaikki työntekijät. Tietotarpeet eri johtotasoilla luonnollisesti vaihtelevat ja ne tulee ymmärtää osana tietoturvallisuuden johtamista. Korkeimmilla johtotasoilla tietotarpeet tietoturvallisuudesta liittyvät rahaan ja tietoturvallisuuden tilaan kokonaisuudessaan. Tietohallintojohtaja tarvitsee työssään tietoa siitä, kuinka hyvä tietoturvallisuuden tila on ja mitkä ovat sen aiheuttamat kustannukset. Tietohallintojohtajan tulee myös ymmärtää, mitä vaatimuksia tietoturvallisuus aiheuttaa esimerkiksi tietojärjestelmille tai muille IT-palveluille. Liiketoimintajohtajat tarvitsevat kustannusten ja yleisen tietoturvallisuuden tilan lisäksi tietoa tietoturvallisuuden suorituskyvystä, eli siitä miten tietoturvallisuus vastaa sille asetettuihin tavoitteisiin suunnitellulla tavalla. Muut roolit, kuten tietojärjestelmäarkkitehti, ohjelmistokehittäjä ja testaaja, tar-

vitsevat työssään enemmän tietoa tietoturvavaatimuksista, niiden toteutustavoista, tietoturvaperiaatteiden mukaisista työskentelytavoista ja käytännön uhista kuin siitä miten yrityksen tietoturvaa kokonaisuutena hallitaan. (Savola 2010.) Nämä tietotarpeet ovat yleistyksiä, jotka sopivat eri aloilla toimivien yritysten tietoturvallisuuden johtamisrakenteen kuvailuun. Niistä voidaan päätellä, että tietoturvallisuus kuuluu osaksi liiketoimintajohtamista, mutta sen päivittäinen huomioiminen on erikseen nimettyjen henkilöiden vastuulla. Mittarit ovat yksi keino, jolla johdon tietotarpeita voidaan täyttää. Tietotarpeita tulee täyttää, sillä johdolla on vastuu yritysten tietopääoman suojaamisesta.

2.3.2 Riskien hallinta osana tietoturvallisuutta

Ylimmän johdon vastuulla on varmistaa ja toteuttaa riittävät toimenpiteet siitä, että organisaation riskejä hallitaan ja niiden vaikutuksia pyritään minimoimaan hyväksyttävälle tasolle. Riskien vaikutuksia käsitellään usein liiketoiminnan häiriöiden kustannuksina. Vaikutuksien näkökulmasta ennakoidaan sitä, miten jonkin riskin toteutuminen vaikuttaa tai häiritsee liiketoimintaa ja siten aiheuttaa kustannuksia esimerkiksi käyttökatkojen ja korjaustoimenpiteiden muodossa. Vaikutusten todennäköisyys on toinen tekijä, jonka perusteella riskejä arvioidaan. Todennäköisyys voi olla esimerkiksi se, että epätoivottu asia tapahtuu kerran vuodessa. (Krutz & Vines 2004, s. 24-25; Brotby 2009, s. 125-126.) Ozier (2004) tiivistää riskien hallinnan tarkoittavan uhkakuvien etsimistä, niiden vaikutusten arvioimista ja uhkakuvien toteutumisen tiheyden arviointia. Lisäksi tulee pohtia, kuinka varmoja riskeihin liittyvistä asioista ollaan. Jos ylin johto määrittelee, että tietyt tapahtumat, joiden kustannukset ovat alle jonkin raja-arvon ja jotka tapahtuvat kerran vuodessa, eivät vaadi toimenpiteitä, saa tietoturvapäällikkö selkeän raja-arvon tai tavoitteen toiminnalleen ja tietoriskien arvioinnille (Brotby 2009, s. 126).

Brotbyn (2009, s. 108) mukaan tietoturvallisuuteen liittyvien riskien vaikutuksia on haastava arvioida. Esimerkiksi käyttökatkojen aiheuttamat saatavuusongelmat muutetaan rahalliseksi niihin kuluneen ajan perusteella, mutta todennäköisyyttä näille on vaikea arvioida. Toisaalta se, mikä jonkun tietovuodon rahallinen arvo on, on liki mahdoton tietää varsinkin, jos organisaatio ei ole määritellyt eri tiedoille arvoja. Todennäköisyyttä on vaikea pohtia, sillä tietovuoto voi tapahtua monella eri tavalla. Myös Savola et al. (2012) mainitsevat, että tietoriskejä on yleisesti vaikea ennustaa ja uusia uhkia tietoturvallisuudelle muodostuu jatkuvasti. Lisäksi huonosti määritellyt tietoturvallisuuden tavoitteet ja eri käsitykset tietoturvallisuuden tilasta organisaatiossa muodostavat haasteita riskien hallinnalle.

Riskien arviointi on ensimmäinen osa prosessia, jonka perusteella tehdään investointeja tietoturvallisuuteen (Pettigrewn 2012). Jaquithin (2007, s. 99) mukaan tietoturvallisuuden näkökulmasta riskejä tulee arvioida sen mukaan, miten hyvin organisaatio tuntee sen teknologiaan, henkilöstöön ja prosesseihin liittyvät riskit. Usein tieto siitä, että tiedetään mitä ei tiedetä, auttaa tietoriskien hallinnassa. Tällöin voidaan tunnistaa potentiaalisia uhkia tietoturvallisuudelle tai aukkoja tietoturvatoimenpiteiden muodostamissa

suojausmenetelmissä. Tässä menetelmässä ei muodosteta mittareita riskien arviointiin, vaan pyritään ymmärtämään riskien arviointiprosessia. Riskiarviota ei muodosteta, sillä arvio riskin suuruudesta on aina vahvasti subjektiivinen. Jaquith (2007, s. 101) mainitseekin, että tehokkain keino tietoriskien hallinnalle on yksinkertaisesti mitata, kuinka monelle tietoresurssille suoritettu riskien arviointi.

Krutzin & Vinesin (2004, s. 28) mukaan riskien arviointi tarkoittaa arvioita siitä, mitä tietoa organisaatio menettää eri tietoresurssien kautta. Tämän jälkeen voidaan arvioida, mitä mahdollisia uhkia tietoresursseihin liittyy. Lopulta määritetään arvo eri tietoresurssien riskeille. Kun tietoresurssien arvot lasketaan yhteen, saadaan kokonaisarvio siitä, mitä esimerkiksi vuoden aikana saatetaan menettää tietoturvallisuuteen liittyvien riskien toteutuessa. Jaquithin (2007, s. 101) mukaan subjektiivisuuteen perustuvat mittarit eivät välttämättä kerro totuutta riskeistä. Näin ollen arvon määrittäminen ei välttämättä ole tietoriskien kannalta olennaista. Tosin organisaation ylin johto käsittelee riskejä usein rahassa mitattuna, jolloin jokin menetelmä riskien arvottamiselle olisi varmasti tärkeä. Pettigrewn (2012, s. 162) mukaan riskien arvioinnin tavoitteena on tuottaa ymmärrystä, jonka avulla organisaation riskejä kuvaillaan, mitataan, pienennetään ja hallitaan.

Arvioinnin jälkeen tulee päättää, mitä löydetyille riskeille tehdään, eli miten niitä pienennetään ja hallitaan. Brotbyn (2009, s. 103) mukaan hyväksyttäviä riskejä, eli niitä joiden suhteen päätetään olla tekemättä mitään, pitää tarkkailla ja havaita, mikäli niistä kasvaa sellaisia riskejä joihin tulee reagoida. Tällaisia riskejä pienennetään lisäämällä kontrolleja tai kehittämällä tietoturvatoimintoja. Tärkeimmät tietoriskien hallintaan liittyvät päätökset koskevat riskiä pienentävän tietoturvatoiminnon hankintaa ja arvioita sen tuoman suojauksen tasosta (Brotby 2009, s. 108). Muita tietoriskien hallinnan päätöksiin vaikuttavia tekijöitä ovat esimerkiksi:

- Tietotoresurssin kriittisyys ja herkkyys
- Tietoresurssin menettämisestä, rikkoutumisesta tai varastamisesta johtuvat vaikutukset
- Tietoon kohdistuvien uhkien laajuus
- Organisaation strategiaan liittyvät suunnitelmat
- Hyväksyttävä riskitaso

Riskien hallinta tarjoaa tietoturvallisuudelle keinon, jolla siihen liittyviä riskejä voidaan arvioida perinteisempien riskien ohella. Riskien hallinnan avulla tietoturvapäällikkö pystyy määrittelemään tietoturvallisuuden toimintoja, jotka liittyvät liiketoiminnan tavoitteiden täyttämiseen. Tietoriskien hallinnan kautta määritellään kustannustehokkain ja viisain tapa, jolla liiketoimintaan liittyvää tietoa suojataan. (Brotby 2009, s. 108-109.) Tietoriskit voidaan riskien hallinnan menetelmin nostaa esille ja suurimmat niistä päätyvät liiketoimintajohdon ratkaistaviksi. Käytännössä tällaisia riskejä ovat suuren luokan investointeja vaativat riskit, joita tietoturvapäällikkö ei itse pysty hallitsemaan. Todennäköisyyksien ja kustannusten pohtimisen sijaan käytännöllisempää tietoriskien

kannalta onkin pohtia, mitkä järjestelmät ovat mahdollisesti haavoittuvia, mitä uhkia eri tietoihin liittyen havaitaan ja mitkä ovat mahdolliset seuraukset. (Pettigrew 2012, s. 31.)

2.3.3 Tietoturvallisuus tietojohtamisen näkökulmasta

Tietojohtaminen on ala, joka tarkastelee erilaisten organisaatioiden toimintaan, johtamiseen ja kehittämiseen liittyviä ilmiöitä tietoon liittyvien resurssien, prosessien ja teknologioiden roolien ymmärtämisen näkökulmasta. Tietojohtamisen tutkimus tuottaa käsitteitä, malleja ja menetelmiä, joilla organisaatioiden toimintaa voidaan edellä mainitusta näkökulmasta analysoida ja kehittää. (Lönnqvist et al. 2007.) Tietoon liittyvien resurssien ja toimintojen avulla tuotetaan liiketoiminta-arvoa, sillä tieto vaikuttaa eri muodoissaan kaikkeen yrityksen toimintaan. Esimerkiksi asiakassuhteita, innovointia, myyntiä, tapahtumienkäsittelyä ja toimitusketjua ohjataan omilla järjestelmillä. Toisaalta yrityksellä on analyyttisia sovelluksia, joiden koostaman informaation pohjalta tehdään liiketoimintakriittisiä päätöksiä. Näitä päätöksiä ja muita organisaation tehtäviä tehdään tietämyksen ja osaamisen avulla. (Kaplan & Norton 2004, s. 207, 251). Tietojohtamisen tavoitteena on kehittää liiketoiminnan suorituskykyä parantamalla tiedon käyttöä ja hyödyntämistä. Tietoturvallisuus taas pyrkii turvaamaan organisaation tietojen käyttömahdollisuudet, jotka määritellään tavallisesti eheyden, luottamuksellisuuden ja saatavuuden avulla.

Pekkola (2012) kuvailee tietojohtamisen näkökulmasta, että organisaation keräämän tiedon laatu heikkenee väistämättä, mikäli sille ei ole nimetty omistajaa. Tiedon laadun heikkenemisellä tarkoitetaan tässä yhteydessä sitä, että tiedosta tulee virheellistä, vaillinaista, epärelevanttia tai vanhaa, jos kukaan ei seuraa sen laatua tai vastaa ylläpidosta. Toisin sanoen Pekkola esittelee yhden mekanismin, jolla organisaation tiedon eheys vaarantuu. Luotettavuuden ja saatavuuden varmistaminen ovat osaltaan lähellä liiketoimintatiedonhallintaa. Liiketoimintatiedonhallinnalla pyritään kehittämään organisaation kilpailukykyä siten, että tarjotaan ennakoitavuutta, nopeaa päätöksentekoa ja mahdollisimman monipuolisia keinoja tiedon hyödyntämiseen. Tämä toteutetaan teknologian avulla siten, että datalle annetaan merkityksiä sekä jalostamalla ja puhdistamalla sitä tukemaan päätöksiä. (Pirttimäki 2007.) Liiketoimintatiedonhallinnalla avulla pyritään siis tarjoamaan oikeaan aikaan oikeaa tietoa oikealle henkilölle. Toisin sanoen suuresta määrästä dataa pyritään löytämään ja hyödyntämään vain eheää ja päätöksenteolle relevanttia tietoa, joka pyritään pitämään mahdollisimman saatavilla sen käyttöön valtuutetuille. Eheyden varmistaminen on tärkeää osana liiketoimintatiedonhallintaa, sillä vaillinaiseen tietoon perustuvat päätökset, jotka liittyvät esimerkiksi taloudellisiin asioihin, voivat olla riski organisaatiolle.

Tietoturvallisuuden tekninen toteutus on puhtaasti tiedonhallintakeinoja suojaava elementti. Esimerkiksi luvussa 2.2 esitellyt tietoliikenneturvallisuus, ohjelmistoturvallisuus ja laitteistoturvallisuus pyrkivät siihen, että organisaation eri järjestelmät toimivat suunnitellusti, niiden välinen kommunikointi toimii ja niistä voivat etsiä tietoa vain ne jotka

sitä tarvitsevat ja ovat oikeutettuja sen käyttöön. Tietoturvallisuuden osa-alueista tietoaineistoturvallisuus taas on edellisessä kappaleessa kuvatun mukaisesti lähimpänä tietojohtamista. Tietoaineistoturvallisuuden näkökulmaan kuuluu tietojen omistajuus ja sen kautta tiedon luokittelu sekä käsittelyohjeet, joiden avulla varmistetaan että tiedon laatu ei heikkene. Tietoturvallisuus suhtautuu tietojohtamiseen osittain sen tukifunktiona, eli tiedon käytön tehokkaamman hyödyntämisen varmistajan ja suojaajana. Toisaalta osa tietoturvallisuuteen liittyvistä menetelmistä on hyvin samankaltaisia, kuin tietojohtamiseen ja varsinkin tiedonhallintaan liittyvät asiat. Joka tapauksessa voidaan nähdä, että tietoturvallisuus on olennainen osa kokonaisvaltaista ja hyvää tietojohtamista.

Aineeton pääoma ja sen mittaaminen on yksi tietojohtamiseen liittyvä aihepiiri, joka muistuttaa tietoturvallisuuden mittaamista. Esimerkiksi informaatiopääoma ja inhimillinen pääoma ovat aineettoman pääoman osa-alueita, joiden kautta voidaan pohtia, minkälaisia aineettomia tietoresursseja yrityksessä on sekä mikä on niiden toivetila ja nykytila (Kujansivu et al. 2007, s. 45). Tällainen pohdinta sopii tietoturvallisuuden osa-alueisiin, joista osa, esimerkiksi ohjelmistot, tietoliikenne ja tietoaineistot, on aineetonta pääomaa. Tietoturvallisuus, ja varsinkin siinä tehdyt virheet, näkyvät Kujansivun et al. (2007, s. 179) esittelemissä aineettoman pääoman mittareissa, jotka mittaavat asiakastyytyväisyyttä ja brandia. Myös muut mittarit voivat antaa viitteitä tietoturvallisuuden tilasta, mutta niitä ei voida suoranaisesti kutsua tietoturvamittareiksi. Esimerkiksi teknologian hyödyntämiseen, osaamiseen ja informaation hallintaan liittyvistä mittareista voidaan päätellä tietoturvallisuuteen liittyviä asioita tai niiden yhteyteen on mahdollista liittää tietoturvamittareita.

2.4 Tietoturvastrategia ja tietoturvapolitiikka

Kairab (2005) näkee tietoturvastrategian organisaation tietoturvallista toimintaa ohjaavana elementtinä. Tietoturvastrategia perustuu liiketoiminnan tarpeisiin ja vastaa osaltaan liiketoiminnan jatkuvuuden turvaamisesta, tietojenkäsittelyn laadukkuudesta jokaisen tiedon ulottuvuuden suhteen ja tietoriskien arvioinnista. Tietoturvastrategiaa laatiessa tulee tunnistaa liiketoiminnan näkökulmasta relevantteja riskejä ja esittää ne selkeällä tavalla, jotta ne voidaan liittää tietoturvapolitiikkaan ja ohjeistuksiin. Tämä toteutetaan käytännössä tunnistamalla organisaatiolle tärkeä tieto ja toiminnalle kriittiset järjestelmät sekä arvioimalla, mikä vaikutus liiketoiminnalle on, mikäli näiden luottamuksellisuus, eheys tai saatavuus vaarantuu. (Kairab 2005, s. 45-46.) Kairab ei huomioi informaation tai tietämyksen turvaamista osana strategian laatimista, mutta Desouza (2007, s. 9) huomauttaa, että yhteistyökumppaneiden, ulkoistuskumppaneiden ja asiakkaiden kanssa tietoa jaetaan muilla tasoin kuin vain datana. Voidaankin päätellä, että osana tietoturvastrategiaa tulee tunnistaa myös informaatio ja tietämys, jota käytetään osana liiketoimintaa, mutta halutaan pitää luottamuksellisena, eheänä ja saatavilla.

Strategiaa kartoitettaessa on huomioitava kustannustehokkuus. Hare (2005) huomauttaa, että organisaation tietojen suojaaminen ei saa ylittää suojattavan tiedon arvoa. Tästä voidaan päätellä, että tietoturvastrategiaa suunniteltaessa ei voida tavoitella täydellistä suojaamista, sillä se olisi kustannustehotonta. Baskerville & Dhillon (2008) mainitsevatkin kustannustehokkuuden näkökulmasta tietojen suojaamisen määrän ja laadun, jotka osaltaan vaikuttavat myös tietoturvallisuuden kustannuksiin. Mitä paremmin tietoja suojataan, sitä vaikeampi niihin on päästä käsiksi, jolloin käytettävyys kärsii samalla huomattavasti. Tietoturvallisuuden tavoitteena ei ole suojata kaikkia tietoja, vaan tukea ja suojata liiketoimintaa. Tietoturvallisuus ei saa hidastaa tai vaikeuttaa liiketoimintaa, vaan sen on samalla sekä mahdollistettava että turvattava liiketoiminnan sujuvuus ja jatkuvuus. Tietoturvallisuuteen liittyviä riskejä on arvioitava samalla tavoin kuin muita liiketoimintaan liittyviä riskejä, jolloin niiden merkitys ymmärretään laajasta näkökulmasta. Kustannustehokkuus muodostuu siitä, että ymmärretään eri liiketoimintayksiköiden tarpeet ja uhat, jonka jälkeen optimoidaan niille sopiva tietoturvataso. (Kayworth & Whitten 2010).

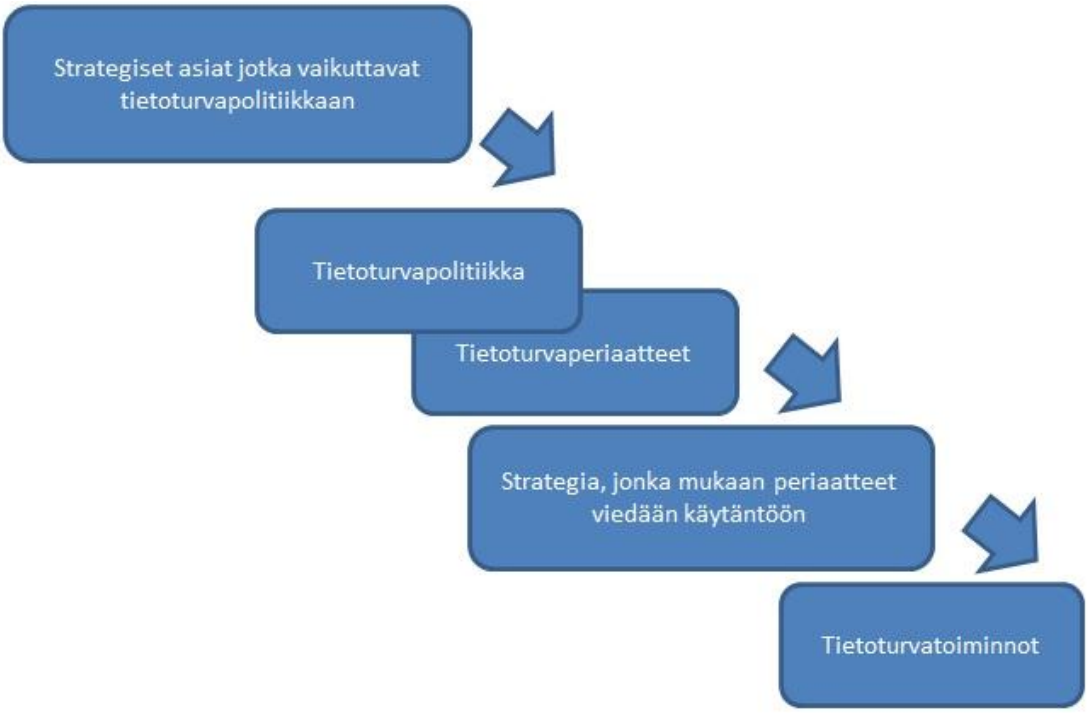
Liiketoimintaan liittyvien tavoitteiden lisäksi tietoturvastrategiaa ohjaa usein lainsäädäntö tai muut normistot. Esimerkiksi henkilötietolaki, laki yksityisyyden suojasta ja laki sähköisestä viestinnästä asettavat velvoitteita organisaation hallussa pitämien tietojen käsittelylle. Esimerkkitapauksena voidaan pitää tilannetta, jossa yritys tavoittelee kustannussäästöjä käyttämällä pilvipalveluntarjoajaa tietojen säilytykseen. Tällöin tiedot saattavat sijaita Euroopan unionin rajojen ulkopuolella, jolloin laki ei välttämättä salli henkilötietojen säilytystä. On myös huomioitava, että laki kieltää henkilötietojen luovuttamisen kolmansille osapuolille. (HTL 22.4.1999/52.) Laki antaa tässä tapauksessa selkeän suuntaviivan organisaation tietoturvallisuudelle ja se on huomioitava osana liiketoimintaa. Yksi suuri vaikuttaja yritysten toimintaan lakien lisäksi on Euroopan Unioni, joka asettaa säädöksiä tietoturvallisuuteen liittyen, tekee tietoturvatutkimusta ja tiedottaa tietoturvauhkista (Enisa 2012). Straub et al. (2008) huomioivat lisäksi muun valtionhallinnon säätelyn ja kansallisen turvallisuuden. Käytännön esimerkki tästä on vakuutusyhtiöitä koskevat erilliset ohjeet, jotka Finanssinvalvonta on luonut operatiivisten riskienhallinnan tehokkuuden varmistamiseksi eläke-, luotto- ja vakuutuslaitoksissa. Tietoturvallisuuden näkökulmasta puhutaan usein vaatimustenmukaisuudesta, johon kuuluvat toimialan vaatimukset ja lain asettamat vaatimukset (Kayworth & Whitten 2010).

Straub et al. (2008) listaavat tietoturvastrategiaa ohjaaviksi tekijöiksi toimialaan liittyvät standardit ja yleisemmin etiikan. Standardit voivat tarkoittaa laatuvaatimuksia, työturvallisuusstandardeja tai järjestelmiin liittyviä ohjeistuksia, kun taas etiikka tarkoittaa kaikkea organisaation työntekijöiden toimintaa. Standardit voidaan myös nähdä kuuluvan osaksi vaatimustenmukaisuutta ja etiikka osaksi organisaatiokulttuuria, jonka mukaisesti henkilökunta usein toimii (Kayworth & Whitten 2010). Tässä tutkimuksessa tietoturvallisuutta esitellään kirjallisuuden lisäksi ISO/IEC 27001 ja valtionhallinnon

tietoturvaohjeiden näkökulmasta. ISO-standardit ovat kansainvälisiä, vapaaehtoisesti käytettäviä vaatimuksia, ohjeita ja toimintamalleja (ISO 2012). Valtionhallinnon ohjeet taas ohjeistavat valtion ja sen käyttämien toimittajien tietoturvatoimintaa (Valtionvarainministeriö 2012). Baskerville & Dhillon (2008) viittaavat useassa kohdassa asiakasvaatimuksiin, jotka ovat vaatimuksia toimitusvarmuudesta, tietojen käsittelystä ja hyväksyttävästä riskitasosta. Tietoturvastrategiaan liittyy myös toimittajanäkökulma, sillä organisaation on tehtävä linjaukset siitä, mitä toimittajien tietoturvallisuudelta vaaditaan ja miten näitä vaatimuksia valvotaan.

Tietoturvastrategia antaa päämäärät ja tietoturvallisuuteen liittyvät tavoitteet tietoturvapolitiikalle, jonka perusteella taas muodostetaan organisaation tietoturvaperiaatteet. Shortenin (2004) mukaan tietoturvallisuuden kehittämisen ensimmäinen askel on politiikan määrittäminen, ei tietoturvastrategian, kuten Kairab (2005) asian esittelee. Baskerville & Dhillon (2008) määrittelevät, että politiikka on lopullinen toiminnan suunnannäyttäjä, jonka sisältö on valittu vallitsevan tilanteen mukaisesti ja jossa on huomioitu organisaation strategia. Kairab (2005) ja Shorten (2004) esittelevät tietoturvapolitiikan dokumenttina, jossa kerrotaan mitä organisaatiossa tulee tehdä, jotta se vastaa strategisiin tavoitteisiin. Hare (2004) taas näkee politiikan kokoelmana toimintoja, joilla organisaatio hallinnoi ja suojaa resurssejaan saavuttaakseen tietoturvatavoitteensa. Whitman (2008) painottaa, että tärkeintä tietoturvapolitiikalle on sen sisällön yhdenmukaisuus lakien kanssa ja se, että tekstin avulla osoitetaan työntekijöiden oikeudelliset vastuut tietoturvallisuudesta. Kaikille yhteinen näkemys on, että tietoturvapolitiikka on organisaation tietoturvallisuuden kivijalka ja johdon viesti siitä, että se ottaa tietoturvallisuuden vakavasti.

Tietoturvallisuuden ulottuvuuksien näkökulmasta tietoturvapolitiikka liittyy usein luotettavuuteen ja eheyteen (Hare 2004, Shorten 2004). Shorten (2004) perustelee tämän sillä, että tietoturvapolitiikan tulee kertoa organisaation jokaiselle työntekijälle mitä he saavat tehdä, mitä ei saa tehdä, mitä pitää tehdä ja mikä heidän vastuu on tietoturvallisuudesta sen luottamuksen ja eheyden suhteen. On kuitenkin huomattava, että työntekijät voivat väärillä toimintatavoilla vaikuttaa saatavuuteen. Esimerkiksi suurten tiedostojen siirto, teräväkuvavideoiden katselu sekä pahimmillaan laiton lataaminen ja jakaminen kuormittavat organisaation tietoverkkoa ja heikentävät siten saatavuutta. Kuvassa 2.2 esitetään tietoturvastrategian ja -politiikan suhde toisiinsa sekä näiden jälkeiset tasot tietoturvan hallinnoinnista.



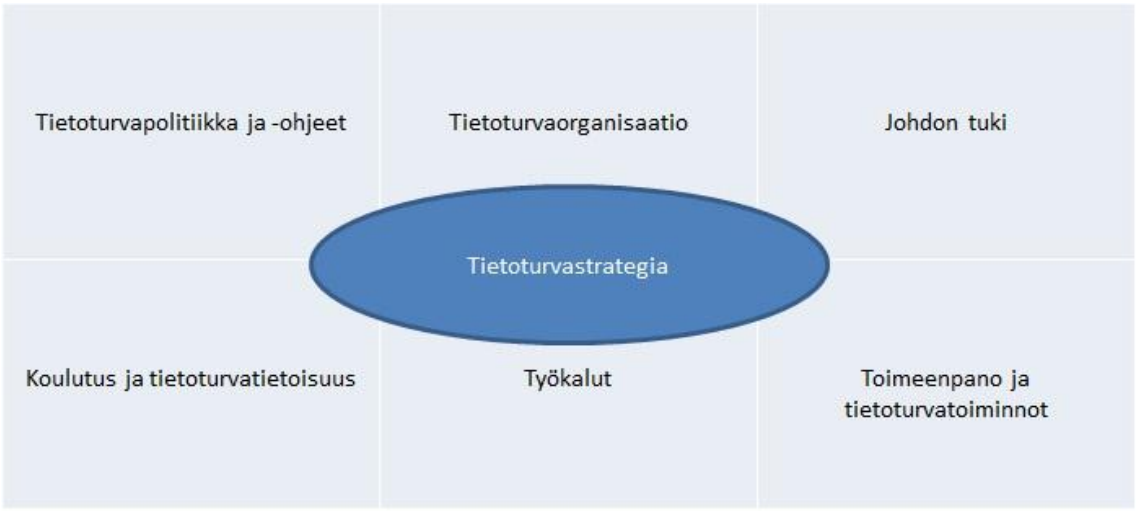
Kuva 2.2. *Tietoturvastrategian tasot. (Mukailtu lähteestä Baskerville & Dhillon 2008)*

Tietoturvastrategia ja tietoturvapolitiikka antavat suuntaviivat organisaation tietoturvallisuuden hallinnoinnille (Baskerville & Dhillon 2008). Tietoturvallisuuden hallinnointiin kuuluu olennaisesti organisaation tietoturvallisuuteen liittyvien periaatteiden määrittely. Tämä tarkoittaa, että organisaation on päätettävä mitä asioita se pitää tärkeinä ja luoda periaatteet miten niiden tietoturvallisuus varmistetaan. Periaatteet muodostetaan tietoturvapolitiikan mukaisesti siten, että ne tukevat organisaation tavoitteita ja sopivat organisaation riskienhallintaan. Riskitaso ja organisaation tavoitteet määrittelevät miten tietoturvallisuutta hallinnoidaan ja kuinka kattavasti organisaation tietoturvallisuus toteutetaan. Kun organisaatiossa on määritelty mitä, miten ja kuinka kattavasti sen tietoturvallisuutta hallinnoidaan, tunnistetaan hallinnointiin liittyviä tekijöitä ja organisoidaan tietoturvatoimintojen toteutusta. (Brotby 2009, s. 83-84.)

2.5 Tietoturvallisuuden hallinnointi

Kairab (2005, s. 45) esittelee tietoturvallisuuden hallinnoinnin tietoturvaohjelmana, johon kaikki tietoturvallisuuteen liittyvät toimenpiteet kuuluvat. Tietoturvallisuuden hallinnointia toteutetaan organisaation tietoturvastrategian määrittelemässä viitekehyksessä, jonka sisältö vaihtelee toimialan ja organisaation mukaan. Kuvassa 2.3 esitellään, miten Kairab huomio tietoturvapolitiikan osana hallinnointia. Kuten edellisessä luvussa esitettiin, tietoturvapolitiikassa esitettyjen asioiden perusteella kehitetään lopulta tietoturvalliset käytännöt ja prosessit. Kuvan 2.3 esittämä tietoturvaohjelma ei ole ristiriidassa kuvan 2.2 kanssa. Tietoturvaohjelma on pikemminkin osa kuvaa 2.2 strategiana, jonka perusteella tietoturvaperiaatteet viedään käytäntöön. Jokaiseen osa-alueeseen voidaan liittää prosesseja ja tietoturvatoimintoja. Esimerkiksi osa-alue ”Tietoturvapolitiikka ja –

ohjeet” sisältää kaksitasoisen näkemyksen. Ensin politiikan avulla luodaan periaatteet siitä, mitä pitää tehdä, jonka jälkeen ohjeet kertovat miten nämä periaatteet toteutetaan käytännössä. Osa-alue ”Tietoturvaorganisaatio” taas vastaa siitä, että politiikat ja periaatteet ovat ajankohtaisia ja toimivat aktiivisesti yhteistyössä johdon kanssa, jotta varmistutaan, että tietoturvakäytännöt ovat strategian mukaiset. Käytännössä tämä tarkoittaa tietoturvallisuustoimintojen toimeenpanoa, joka huomioidaan erikseen osana tietoturvan hallinnointia. Tällä painotetaan sitä, että tietoturvallisuus ei saa jäädä periaatteiden tasolle. (Kairab 2005 s. 47-51)



Kuva 2.3. *Tietoturvaohjelma. (Mukailtu lähteestä Kairab 2005, s. 45)*

Kairab (2005, s. 50-51) huomauttaa johdon tuen olevan tärkeässä osassa tietoturvallisuuden hallinnointia, sillä se tuo perustan kaikelle tietoturvallisuuden hallinnointiin liittyville asioille. Johto määrittelee sallitun riskitason ja ottaa vastuun riskien toteutumisesta, osoittaa menettelytapojen tärkeyden ja varmistaa että ne sopivat organisaation tavoitteisiin. Johto vastaa siitä, että organisaatio toimii lain ja muiden vaatimusten mukaisesti tietoturvallisuuden suhteen. (Brotby, 2009, s. 83; VAHTI 2/2011). Standardi ISO/IEC 27001:fi tiivistää, että johdon tulee tukea turvallisuutta organisaatiossa osoittamalla selkeää suuntaa ja näkyvää sitoutumista sekä osoittamalla tietoturvavastuita. Brotby (2009, s. 83) esittelee johdon olevan lopulta vastuussa siitä, että sen määrittelemät liiketoiminnalliset tavoitteet täyttyvät. Tavoitteiden saavuttamiseksi johdon tulee huomioida, että tietoturvallisuudella on riittävät resurssit (VAHTI 2/2011). Lisäksi johdon tulee varmistua siitä, että organisaation resursseja käytetään asianmukaisesti. Tietoturvallisuuden hallinnoinnin kannalta johdon tulee tukea tietoturvatoimintaa ja omalla esimerkillä osoittaa sen tärkeys. (Desouza 2007.) Johdon tuki on yleisesti tunnistettu kriittinen menestystekijä organisaatiomuutosten, tietojärjestelmähankintojen ja strategisten linjausten yhteydessä (Bourne et al. 2000). Voidaankin päätellä, että holistisen tason tietoturvamittarit tulee suunnitella siten, että niillä mitataan korkean tason tavoitteiden onnistumista.

Tietoturvallisuuden organisointi on yksi keino jakaa vastuita ja varmistaa, että tietoturvallisuus on huomioitu riittävän kattavasti organisaation toiminnassa. Tietoturvaorganisaatio varmistaa, että tietoturvatoimintoja noudatetaan ja että tietoturvallisuuden eri osa-alueisiin liittyviä toimintoja ylläpidetään. Jossain tapauksissa tietoturvaorganisaation muodostaa tietoturvapäällikkö ja tietoturva-analyytikko sekä ryhmä ylläpitäjiä. (Kairab 2005, s. 49.) On huomioitava, että Kairabin (2005) näkemys tietoturvaorganisaatiosta viittaa todella suuren konsernin toimintaan. Esimerkiksi tämän tutkimuksen kohdeyrityksessä, joka on keskisuuri pörssiyhtiö, tietoturvaorganisaatio koostuu kahdesta henkilöstä, mutta tiettyjä rooleja toteutetaan oman toimen ohessa. Au (2012) huomauttaa, että viime vuosina tietoturvapäällikön rooli on muuttunut tekniikka- ja turvallisuuspainotteisesta johtamisesta kohti kokonaisvaltaisempaa tietoturvallisuuden hallinnointia, riskien hallintaa ja vastuunottoa organisaation toimien vaatimustenmukaisuudesta. Liiketoiminnan näkökulmasta tietoturvaorganisaation tulee varmistaa, että tietoturvallisuus on huomioitu liiketoimintaprosesseissa ja järjestelmien kehitysprojekteissa riittävän kattavasti ja se on ajan tasalla (Kairab 2005, s. 50; VAHTI 2/2010). Tietoturvamittarit ovat tästä näkökulmasta johdon päätöksen tekoa tukevia työkaluja, jolla se varmistaa että tietoturvallisuutta hallinnoidaan tavoitteen ja annettujen resurssien mukaisesti.

Tietoturvapolitiikka ei itsessään ole organisaation tietoturvallisuutta lisäävä tekijä, eikä hyvinkään organisoitu tietoturvallisuus ole tae siitä, että organisaatiossa noudatetaan tietoturvaperiaatteita. Organisaatiossa ei voida olettaa, että työntekijät ottavat automaattisesti vastuuta tietoturvasta. (Kairab 2005, s. 51-52.) Whitmanin (2008) mukaan koulutuksen avulla osoitetaan henkilöstön vastuu alueet tietoturvallisuudesta. Koulutus voidaan jakaa kahteen osaan, tietoturvatoimintojen käytön ohjeistukseen, joka sisältää roolikohtaisten tietoturvavastuiden koulutuksen, ja tietoisuuden ylläpitoon, jossa tietoturvallisuuteen liittyviä periaatteita tuodaan aktiivisesti esiin organisaatiossa. (Kairab 2005; Whitman 2008). Toimintojen ohjeistamisen ja tietoisuuden lisäämisen tavoitteena on kouluttaa työntekijät käsittelemään organisaation tietoa tietoturvaperiaatteiden mukaisesti. Näin minimoidaan riski siitä, että tieto häviää, joutuu vääriin käsiin tai tiedon eheys vaarantuu vahingossa tai väärinkäytön seurauksena. (Whitman 2008.) Tietoturvakoulutus on olennainen osa henkilöstöturvallisuutta, jolla pyritään ennakoiden välttämään väärinkäytöksiä (VAHTI 2/2008). Organisaatiolla voi usein olla ongelmana tietää, kuinka hyvin koulutus tukee tietoturvatietoisuutta ja kuinka hyvä tietoturvatietoisuus sen henkilöstöllä on. Mittaamalla näitä asioita ymmärretään, kuinka hyvin henkilöstö tukee ja tuntee organisaation tietoturvallisuutta.

Kairab (2005, s. 53) esittelee tietoturvallisuuteen liittyvät työkalut tietotekniikan näkökulmasta. Tämä näkökulma on jokseenkin perusteltu, sillä tiedonsiirto, tallennus ja muokkaus tapahtuvat tietotekniikan avulla. Esimerkiksi heikkouksien etsiminen tietotekniikkainfrastruktuurista, palvelinten päivitysten ja asetusten automaattinen tarkastaminen ja lokien tutkiminen voidaan tehdä työkaluilla. (Kairab 205, s. 53.) Tällöin varmistetaan, että organisaation tiedonsiirto toimii tietoturvaperiaatteiden mukaisesti eikä

päästä vihollismielisiä tahoja sisään. Tämän lisäksi pyritään varmistamaan, että tieto säilyy palvelimilla turvallisesti. Lokien avulla nähdään poikkeamia tiedon käsittelyssä. Whitman & Mattord (2011, s. 374-380) mainitsevat kryptografisten työkalujen, digitaalisten allekirjoitusten ja sertifikaattien ja tietoteknisten avainten hallinnan kuuluvan olennaisesti tietoteknisen turvallisuuden työkaluihin. Tietoturvallisuuden hallinnoinnin näkökulmasta organisaation tulee tunnistaa mitä työkaluja se hyödyntää ja millä laajuudella, sekä muodostaa periaatteet näiden käytöstä. Muita, ei teknisiä, työkaluja ovat koulutukset, tietoturvan arviointikierrokset ja prosessit liittyen esimerkiksi tietoturvatapahtumien käsittelyyn ja raportointiin (Kwon & Johnson 2012). Tietoturvallisuuden mittaamisella voidaan varmistua, toimivatko työkalut ja tietoturvatoiminnot oikein sekä raportoida johdolle tietoa tietoturvallisuuden tilasta. Mittareiden toteutuksesta vastaa kuvan 2.3 viitekehyksessä tietoturvaorganisaatio.

Tietoturvatapahtumien havainnointi on tärkeä osa tietoturvallisuuden hallintaa. Havainnointia tuetaan organisaation laajuisilla raportointikäytännöillä sekä muodostamalla kanavia sujuvan kommunikoinnin tueksi. Organisaation laajuisen raportoinnin avulla havainnoidaan tehokkaasti tietoturvaongelmia, uhkia ja muita tapahtumia. Osana raportointikäytäntöjä on huomioitava raportointi myös liiketoiminnalta tietoturvallisuudesta vastaaville henkilölle, sillä heidän tulee olla tietoisia liiketoiminnan suunnittelemista aktiviteeteistä. Liiketoiminta aktiviteettien lisäksi lain ja muiden tahojen asettamien vaatimusten viestiminen läpi organisaation on tärkeää. (Brotby 2009, s. 103.) Tehokkaan havainnoinnin avulla ongelmiin pystytään reagoimaan nopeasti. Kun tapahtumia tietoturvallisuuteen liittyen kerätään ja rekisteröidään, saadaan tietoa mittaamista varten.

Tietoturvallisuuden toimeenpano esitellään usein liiketoiminta johtamiseen liittyvän PDCA-mallin avulla, koska se esitellään ISO/IEC 27001 standardissa. Käytännössä malli on holistinen kuvaus siitä, miten tietoturvallisuuden hallintajärjestelmä ja siihen liittyvät prosessit viedään käytäntöön. Mallin ensimmäisessä ”Plan”-vaiheessa luodaan tietoturvallisuuden hallintajärjestelmä, eli käytännössä määritellään tietoturvapolitiikka ja sen kautta kaikki tietoturvallisuuden sateenvarjon alle kuuluvat asiat. Tämän jälkeen ”Do”-vaiheessa toteutetaan ja otetaan käyttöön tietoturvatoiminnot, prosessit ja menettelytavat. Kolmannessa, ”Check”-vaiheessa arvioidaan, kuinka hyvin tietoturvallisuus toteutuu organisaatiossa. Tässä kohdassa tietoturvamittarit ovat erityisen tärkeitä apuvälineitä. Mittaustuloksia tulisi esitellä johdolle, jotta voidaan siirtyä ”Act”-vaiheeseen, eli tietoturvallisuuden parantamiseen, mittaustulosten perusteella. Toiminnan parantaminen vaatii taas siirtymisen ensimmäiseen vaiheeseen, eli suunnitteluun. PDCA-malli on siis jatkuvaan parantamiseen liittyvä prosessi, jonka syötteenä on tietoturvallisuus vaatimukset ja odotukset ja jonka tuotoksena on hallittu tietoturvallisuus. (ISO/IEC 27001:fi)

2.6 Miksi tietoturvallisuutta kannattaa kehittää?

Tietoturvallisuuteen liittyviä uhkia esiintyy jatkuvasti ja suuren luokan tietomurtoja tapahtuu tasaisin väliajoin. Rashid (2012) kertoo artikkelissaan tietoturva-ammattilaisten paneelikeskustelun päätyneen lopputulokseen, jonka mukaan samalla kun tietoturvallisuus kehittyy, kehittyvät vihollismieliset tahot nopeammin. Aiheen tiimoilta artikkelissa todetaan, että on erittäin tärkeää kehittää tietoturvallisuutta kouluttamalla henkilökuntaa ja panostaa organisaation tietoturvallisuudesta vastaavien henkilöiden osaamiseen. Tämän lisäksi johdon tulee ymmärtää kokonaiskuva ulkoistettujen palveluiden, tietoturvaroolien ja liiketoimintaan liittyvien määräysten kannalta. (Rashid 2012.) Wilson (2012) esittelee artikkelissaan Rashidin artikkelia tukevan näkemyksen, jonka mukaan loppukäyttäjät eivät osaa käsitellä henkilökohtaista dataa ja ymmärrä mitä tietoa tulisi suojata. Tämä helpottaa huomattavasti vihollismielisten hyökkäysten toteuttamista. Heimerl (2012a) on tutkinut tietovuotoja ja tiivistää, että yleisimpiä syitä yritysten kokemien tietomurtojen lisäksi ovat työntekijöiden tekemät vahingot, jotka johtuvat tietoturvatietoisuuden puutteesta, teknisten taitojen puutteesta tai virhearvioinneista. Vaikkei Wilsonin ja Heimerlin esittelemillä tutkimuksella ole tieteellistä arvoa, antavat ne näkökulman myös organisaation työntekijöiden tiedon käsittelyyn ja tarpeelle sen turvallisuuden kehittämisestä.

Wianderin (2007) mukaan tietoturvallisuuden kehittäminen lisää ymmärrystä tietoturvallisuudesta ja siihen liittyvistä käytännöistä kaikissa työntekijäryhmissä. Laajentunut ymmärrys tietoturvallisuudesta on tärkeä syy tietoturvallisuuden kehittämiselle, sillä yhdessä teknisten ratkaisujen kanssa se luo perustan organisaation suojattavien kohteiden, prosessien ja resurssien suojaamiselle. Työntekijöillä on viimekädessä mahdollisuus ylläpitää organisaation tietoturvallisuutta ja havaita mahdollisia uhkia ja tietoturvarikkomuksia päivittäisen työnteon ohessa. Organisaation tarpeiden mukainen suojautuminen, tietoturvatietoisuuden lisääminen ja oman toiminnan tunteminen mahdollistavat organisaation toiminnan tietoturvallisuuden ja jopa ennalta ehkäisevät hyökkäyksiä. Organisaatiolla tulee olla sellaiset käytännöt, jotka auttavat henkilöstöä havaitsemaan, ilmoittamaan ja saamaan palautetta tehdyistä havainnoista. Näin organisaatiolla on mahdollisuus oppia ymmärtämään omaa tietoturvallisuuttaan ja siihen liittyviä riskejä. Jos hyökkääjä tuntee organisaation paremmin kuin organisaatio itsensä, hyökkääjän todennäköisyydet onnistua toimissaan ovat todella hyvät.

Tietoa siirtyy yhä enemmän organisaatioiden välillä ja niiden sisällä. Tämän lisäksi tiedon arvo kasvaa. Vihollismielisen toiminnan lisäksi kolmansien osapuolien vaatimukset tiedon käsittelyyn antavat painetta tietoturvallisuuden kehittämiselle. Esimerkiksi asiakkaat saattavat antaa vaatimuksia, jotka organisaation tulee täyttää ennen kaupan tekoa. Toisaalta organisaatio voi käyttää tietoturvallisuutta myyntikeinona ja erikoistua kumppanina, joka huolehtii omista ja asiakkaiden tiedoista. Tiedosta on tullut tärkeä kilpailutekijä, jota tulee suojata ja jonka turvallisesta käsittelyssä on eroja organisaatioiden vä-

lillä. (Wiander 2007.) Mikäli organisaatio ei toimi tietoturvallisesti tai on huolimaton sen suhteen, voi seurauksena olla muutakin kuin kilpailuedun menetys liiketoiminnalle tärkeiden tietojen menetyksen johdosta. Heimerl (2012b) mainitsee esimerkkeinä sakkorangaistukset, maineen menetyksen, oikeudenkäynnit ja vakuutusten menettämisen tai kallistumisen. Jos organisaatio ei tee niitä asioita, joita sen tulisi tehdä liiketoimintaympäristön tietojen suojaamiseksi, se altistuu hyökkäyksistä ja tietomurroista johtuvien uhkien lisäksi myös kolmansien osapuolten langettamille sanktioille.

Tietoturvallisuutta kannattaa siis kehittää, jotta voidaan suojautua organisaation tietoon kohdistuvilta uhilta ja jotta voidaan vastata kolmansien osapuolten asettamiin vaatimuksiin ja välttyä niihin liittyviltä sanktioilta. Kuinka paljon tietoturvallisuutta sitten kannattaa kehittää? Heimerlin (2012b) mukaan tietoturvallisuudella ei ole ”parhaita käytäntöjä”, sillä turvallisuutta voidaan parantaa loputtomiin lisäämällä toimintoja, esimerkiksi estoja, tarkastuksia ja kieltoja. Heimerlin ajatuksen taustalla on tarkoituksenmukaisuuden huomioiminen tietoturvallisuutta kehitettäessä. Kuten tietoturvastrategiaa esiteltäessä mainittiin, kustannustehokkuus ja tarpeenmukaisuus ovat tietoturvallisuuden kannalta tärkeässä roolissa. Tietoturvallisuuden parhaat käytännöt eivät siis viittaa parhaaseen mahdolliseen suojaan vaan tietoturvatoimintojen optimaaliseen hyödyntämiseen. Demetz & Bachlechner (2012) mainitsevat esimerkkinä, että 100 euron arvoista lukkoa ei kannata laittaa 50 euron arvoiseen kohteeseen. Tietoturvainvestoinnit suojaavat ja pienentävät kuluja jotka aiheutuvat tietomurroista. Toinen näkökulma kustannustehokkuuteen on työnteon tuottavuuden parantaminen organisoimalla tietoturvallisuus siten, että henkilöstön ei tarvitse käyttää siihen aikaa päivittäisessä työnteossa poikkeustapauksia lukuun ottamatta. Tämä tarkoittaa esimerkiksi automaattista varmuuskopiointia, sujuvia pääsynhallintakeinoja ja hyvin kontrolloitua tietoliikenneturvallisuutta. Voidaankin päätellä, että tietoturvallisuutta kehittämällä parannetaan tietoturvatoimintojen vaikuttavuuden lisäksi myös kustannustehokkuutta, mikäli löydetään kohteita joiden suojaamisen voisi toteuttaa kevyemmin tai pystytään parantamaan työn tuottavuutta.

Brotbyn (2009, s. 53) mukaan organisaatiot, joiden tietoturvallisuuden tila on keskimääräistä heikompi, kärsivät suurempia tappioita tietomurtojen tai tiedonkäsittelyyn liittyvien virheiden tapahtuessa. On kuitenkin huomioitava, mitkä ovat kustannukset, mikäli organisaatiossa toteutetaan keskimääräistä parempaa tietoturvallisuutta. Toisin sanoen suvereenin tietoturvallisuuden ylläpitäminen voi olla kallista ja ylittää tietoturvavirheiden aiheuttamat kustannukset. Toisaalta organisaatiota on hankala vertailla keskenään, jolloin ei voida varmasti määritellä tietoturvallisuuden tilaa tai eroja eri organisaatioiden tietoturvatoiminnassa. Myös liiketoiminta-alueissa on eroja ja jotkut alat kokevat aina suurempia tappioita kuin toiset. (Brotby 2008, s. 53). On myös huomioitava, että tietyillä aloilla, kuten sairaanhoidossa, poliisitoiminnassa tai puolustusvoimissa, tiedot eivät yksinkertaisesti saa vaarantua. Seuraavassa luvussa paneudutaan mittaamiseen, jonka avulla organisaation tietoturvallisuuden tehokkuudesta ja vaikuttavuudesta saadaan päätöksentekoa tukevaa informaatiota.

3 MITTAAMINEN JOHTAMISEN VÄLINEENÄ

Mittaaminen on tärkeä osa johtamista ja organisaation toiminnan arviointia, sillä sen avulla organisaatio kykenee hallitsemaan ja kehittämään asioita, jotka se on määritellyt tärkeiksi. Tässä luvussa esitellään mittaaminen organisaatiossa ja pohditaan miten se tukee johtamista. Mittaamista ei sen laajuuden vuoksi esitellä kaikilta osin, vaan käydään läpi miten sen avulla voidaan vaikuttaa organisaation suorituskykyyn ja organisaation menestystekijöihin. Näin saadaan näkemys siitä, miten mittarit liitetään osaksi johtamista. Liiketoimintanäkökulmaa mittaamiseen haetaan tasapainotetun mittariston avulla, johon liitetään tietoturvallisuuden menestystekijöitä. Luvun lopuksi esitellään mittariston suunnitteluprosessi, joka sopii myös tietoturvamittaristoprojektin lähtökohdaksi.

3.1 Suorituskyvyn mittaaminen organisaatiossa

Mittarit ovat konkreettisia johtamisen työkaluja. Mittareiden avulla voidaan hallita monimutkaisia kokonaisuuksia, kun mittauksen tuloksia tiivistetään tunnuslukujen muotoon. (Kujansivu et al. 2007, s. 159.) Ylisirniö (2011, s. 175) jaottelee mittaamisen menneisyyden, nykyhetken ja tulevaisuuden mittaamiseen. Menneisyyden mittaaminen tarkoittaa operatiivisen tehokkuuden ja teknisten toimintojen mittaamista ja tulevaisuuden mittaaminen visionääristä skenaarioiden luomista ja simulointia. Näiden välissä on strateginen mittaaminen, joka tarkoittaa nykyhetken mittaamista. Se sisältää vaikuttavuuden ja tehokkuuden mittaamisen sekä strategisten riskien ja painopistealueiden määrittämisen. Strategisen mittaamisen näkökulmana on päätöksenteko, joka samanaikaisesti vaikuttavat sekä nykyhetkeen että tulevaisuuteen. Päätöksiin liittyviä toimintoja mitataan esimerkiksi niiden vaikuttavuuden ja organisaation tehokkuuden suhteen. (Ylisirniö 2011, s. 175-176)

Kaydos (1999) määrittelee suorituskyvyn olevan liiketoiminnan tehokkuuden ja vaikuttavuuden yhdistelmä. Neely et al. (1995) toteavat Kaydoksen tavoin, että organisaation suorituskyvyn taso on sen toteuttamien toimintojen tehokkuuden ja vaikuttavuuden funktio. Vaikuttavuudella Neely et al. (1995) tarkoittavat sitä kuinka hyvin asiakasvaatimukset täytetään ja tehokkuudella sitä kuinka kustannustehokkaasti organisaation resursseja hyödynnetään. Ylisirniö (2011) määrittelee vaikuttavuuden tarkoittavan sitä, kuinka hyvin toteutetut toimenpiteet täyttävät niiden tavoitteenmukaisen funktion. Vaikuttavuuteen kuuluu kaikki epäsuorat tai suorat toimenpiteet, tai tapahtumat, jotka todistettavasti edistävät jonkun tavoitteen täyttymistä Tehokkuus taas tarkoittaa sitä, kuinka hyvin muutos on onnistuttu viemään läpi. (Ylisirniö 2011, s. 176.) Vaikuttavuuden ja

tehokkuuden lisäksi organisaation strategiaa mitataan myös muiden tekijöiden perusteella. Strategian mukaisesti voidaan esimerkiksi muodostaa yksityiskohtaisia toimintasuunnitelmia. Mittareiden avulla seurataan toimintasuunnitelman mukaisten työvaiheiden etenemistä tai suorituskykyä ja viestitään henkilöstölle niihin liittyviä tavoitteita. Tavoitteiden avulla henkilöstöä ohjataan tekemään oikeita asioita, eli toteuttamaan strategiaa. (Kujansivu et al. 2007, s. 160)

Suorituskyvyn mittaaminen tarkoittaa prosessia, jossa toiminnan tehokkuudelle ja vaikuttavuudelle määritellään joku arvo. Suorituskyvyn mittauksessa tarkastellaan yhdelle toiminnolle määriteltyjä arvoja mittarin avulla. (Neely et al. 1995.) Bourne et al. (2000) jakavat suorituskyvyn mittaamisen kirjallisuuskatsauksensa perusteella kahteen ryhmään: strategian implementoinnin onnistumisen arviointi ja strategiaan liittyvien oletamusten haastamisen. Lönnqvistin (2004) mukaan suorituskyvyn mittaaminen on prosessi, jota käytetään mitattavan tavoitteen ominaispiirteen tai ominaispiirteen tilan määrittämiseen. Suorituskyvyn mittaamisella tarkoitetaan siis prosessia, jonka avulla pyritään esittämään, kuinka hyvin tavoitteita ollaan tehokkuuden ja vaikuttavuuden näkökulmasta saavutettu implementoidun strategian kannalta sekä arvioimaan, kuinka hyvin implementoitu strategia vastaa organisaation tarpeita. Tietoturvallisuuden kannalta prosessin syöte voisi olla lain vaatimat tietoturvatoiminnot. Organisaatio voi myös itse asettaa vaatimuksia tietoturvallisuudelle, esimerkiksi standardien mukaisesti. Näiden prosessien toteutumista tai standardien mukaisuutta organisaatiossa mitataan vaikuttavuuden ja tehokkuuden näkökulmasta.

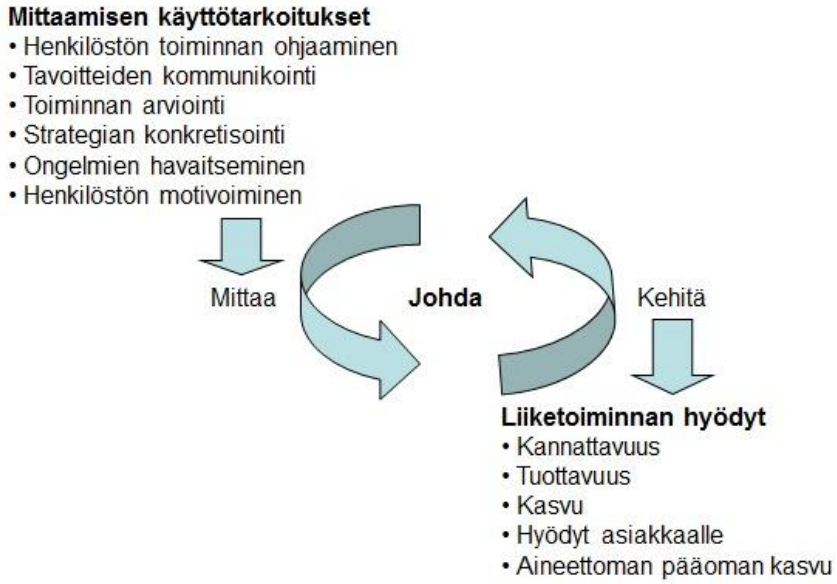
Ylisirniön (2011) mukaan mittaamisen kannalta on tärkeä erottaa ja kategorisoida eri toimenpiteitä toisistaan, jotta ne voidaan liittää eri saavutuksiin. Suorituskyvyn mittaamisen yleisin näkökulma on taloudelliset tekijät tai henkilöstöresurssien käyttö (Packova & Karacsony, 2010). Marr & Schiuma (2003) luettelevat suorituskyvyn mittaamista käsittelevien tieteellisten tutkimusten aihealueiden tulevan laskentatoimen, talouden, henkilöstöhallinnon, johtamisen, markkinoinnin, toiminnanohjaamisen, psykologian ja sosiologian näkökulmista. Organisaation toimintaa siis mitataan mahdollisimman laajaalaisesti, jotta sen toimintaa pystytään arvioimaan mahdollisimman kattavasti. Vaikka taloudelliset mittarit ovat tärkeimpiä suorituskykyyn liittyviä mittareita, johto tarvitsee kattavamman näkemyksen strategian kehittämisen ja toteuttamisen tueksi (Ariyachandra & Frolick, 2008). Sink (1983) huomio, että organisaation suorituskyky on riippuvainen ainakin kannattavuudesta, tuottavuudesta, laadusta, työelämän laadusta ja innovatiivisuudesta. Tietoturvallisuutta ei mainita organisaation suorituskyvyn mittaamista käsittelevissä julkaisuissa.

3.2 Mittaaminen osana johtamisjärjestelmää

Mittaaminen liittyy vahvasti organisaation johtamisen toimenpiteisiin. Johtamisen avulla pyritään ohjaamaan organisaatiota kohti sen tavoitteita. Nämä tavoitteet on ensin

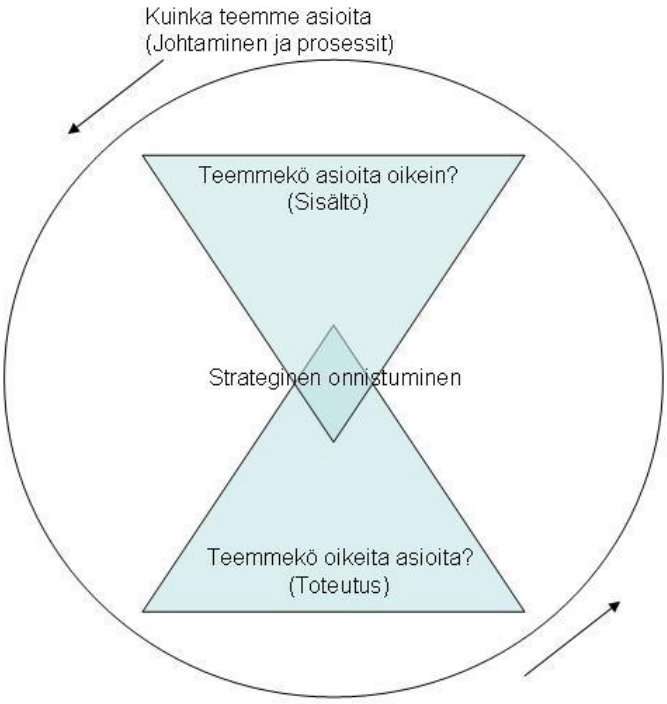
määriteltävä ja pohdittava keinoja, joilla tavoitteisiin päästään. Tämän jälkeen suunnitelmat pitää toimeenpanna ja varmistua siitä, että niitä tehdään oikealla tavalla. Toimintojen tarkkailusta saadaan tietämystä, jolloin voidaan kehittää suunnitelmia ja optimoida tavoitteita yhä paremmin. Johtaminen koostuu siis toiminnan suunnittelusta, toteutuksesta ja tarkkailusta. (Neilimo & Uusi-Rauva 1997, s. 11.) Tässä on selkeä yhteys tunnettuun PDCA-malliin, joka esiteltiin tietoturvallisuuden hallinnoinnin näkökulmasta luvussa 2.5. Mittaaminen on siis tärkeä osa johtamista, jonka avulla tutkitaan ja ymmärretään organisaation toimintaa vertailemalla tuloksia liiketoiminnan asettamiin tavoitteisiin. Tulosten perusteella toimintaa kehitetään, jonka jälkeen mittareiden avulla seurata muutosten vaikutusta.

Saari (2006) kuvailee mittaamisen prosessiksi, jossa toimenpiteet antavat perusteen mittaamiselle ja mittauksen tulos antaa perusteen toimenpiteen muuttamiselle. Mittaaminen on johdon ja johtamisen työkalu, jonka avulla se voi ohjata ja tarkkailla toimintoja, mutta sitä käytetään myös muilla organisaation tasoilla (Lönnqvist 2002, s. 30). Esimerkiksi ylimmän johdon näkökulmasta on tärkeää mitata, miten hyvin organisaatio toteuttaa strategiaansa, kun taas keskijohto hyödyntää suorituskykymittareita arvioidessaan ja motivoidessaan työntekijöitä suorituskyvyn ja tuottavuuden näkökulmasta (Kaplan, 2009). Työntekijän näkökulmasta mittareiden avulla voi seurata ja kehittää omaa toimintaansa (Lönnqvist et al. 2006, s. 123). Kuvassa 3.1 on esitetty johtamisjärjestelmä, sen hyödyt liiketoiminnalle ja mittaamisen käyttötarkoitukset. Henkilöstön toiminnan ohjaaminen ja tavoitteiden kommunikointi ovat tärkeässä roolissa mittaamisessa, jotta muutoksia pystytään toteuttamaan ja mittareita tulkitaan samalla tavalla läpi organisaation. Mittarit ovatkin yksi keino kannustaa henkilöstöä tietynlaisiin suorituksiin. Nämä suoritukset voidaan mittareiden avulla sitoa yrityksen strategiaan ja näin konkretisoida sitä operatiivisen toiminnan tavoitteiksi.



Kuva 3.1. *Mittaamisen käyttötarkoitukset ja johtamisjärjestelmän hyödyntäminen. (Mukailtu lähteistä Lönnqvist 2002 & Kujansivu et al. 2007)*

Ylisirniö (2011, s. 32) perustelee strategisen mittaamisen toiminnan sisällön ja toteutuksen kautta. Sisältö vastaa kysymykseen ”Tekeekö organisaatio oikeita asioita?” ja toteutus ”Tekeekö organisaatio asioita oikein?”. Näitä asioita tarkastellaan johtamisen ja prosessin näkökulmasta. Olennaisena asiana on mitata sellaisia asioita, jotka pitkällä aikavälillä tarkasteltuna vaikuttavat organisaation strategian onnistumiseen ja siihen kuinka hyvin ylimmän tason tavoitteet täyttyvät. (Ylisirniö 2011, s. 31-33.) Kuvan 3.1 esittelemät käyttötarkoitukset jakaa pitkän aikavälin, toiminnan ohjaamisen ja ongelmatilanteisiin reagoiviin mittareihin (Kujansivu 2007, s. 161). Tämän jaottelun voi liittää karkeasti Ylisirniön (2011, s. 22) esittelemään strategian mittaamisen perspektiiviin, joka esitetään kuvassa 3.2. Prosesseja voidaan mitata siten, että ongelmatilanteet tulevat herkästi esille. Toiminnan sisältöä mitataan pikemminkin toiminnan ohjaamisen näkökulmasta ja toteutusta pitkän aikavälin mittareilla. On kuitenkin huomattava, että mittarit voivat tapauskohtaisesti kattaa jopa kaikki edellä mainitut ulottuvuudet. Kuvassa 3.2 tiivistetään Ylisirniön näkökulma siitä, että organisaation toimintaa mitataan, jotta johto pystyy arvioimaan, tekeekö organisaatio oikeita asioita oikealla tavalla.



Kuva 3.2. *Strategian mittaamisen perspektiivi (Mukailtu lähteestä Ylisirniö 2011, s. 22)*

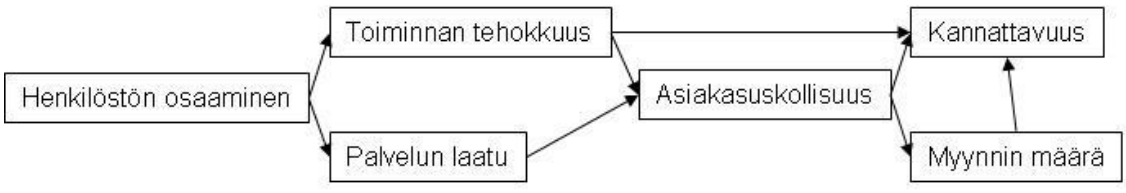
Tietoturvallisuuden näkökulmasta kuvassa 3.2 esitetty strategian mittaamisen perspektiivi ei muutu. Yhtälailla tietoturvallisuuden johtamisen kannalta on tärkeää tietää, suojataanko yritystä tarpeenmukaisesti, eli onnistutaanko toteuttamaan tietoturvastrategiaa. Kuten luvussa 2.6 keskusteltiin, esimerkiksi tietoturvallisuuden kustannustehokkuuden parantaminen on yksi tärkeä kehittämiskohde, jotta resurssit osataan kohdistaa parhaalla mahdollisella tavalla. Tämä ymmärtäminen vaatii tiedon siitä, tehdäänkö oikeita asioita oikealla tavalla. Se, mitä tietoa strategian mittaamisen liittyvistä asioista kannattaa etsiä,

voidaan päätellä Kujansivu et al. (2007 s. 160) esittelemistä syistä mitata organisaation toimintaan, joita ovat esimerkiksi:

- Tuetaan päätöksentekoa tukevaa informaatiota
- Motivoidaan henkilöstöä
- Kyseenalaistetaan toimintatapoja
- Luodaan perusta palkitsemiselle
- Ennakoidaan liiketoiminnan kehitystä
- Opitaan organisaation toiminnasta
- Viestitään yrityksen voimavaroista

Nämä seikat kuvailevat sekä toteutuksen onnistumista että strategian sisällön oikeellisuutta. Ne sopivat myös tietoturvastrategian mittaamisen perusteeksi. Luvussa 2.4 esiteltiin tietoturvastrategian sisältö. Vaatimustenmukaisuuden täyttyminen voisi kuvastaa Ylisirniön (2011, s. 22) esittelemää toteutuspuolta ja sen avulla pystytään tukemaan päätöksentekoa siitä, mitä tietoturvallisuuden osa-alueita tulee kehittää. Luvussa 2.5 esiteltiin tietoturvallisuuden hallinnointia ja käytännön keinoja sen toteutukselle. Tämä taas voisi kuvastaa sisältöpuolta, eli sitä onko organisaatio toteuttanut asioita oikein. Näiden perusteella organisaatio voi kyseenalaistaa toimintatapoja ja mittaamisen kautta oppia uusia asioita organisaation tietoturvatoiminnasta. Johtamisen ja prosessien osuus puolestaan kuvailee kuinka hyviä eri tietoturvatoiminnot ovat ja pystytäänkö näitä hallinnoimaan riittävän hyvin. Tietoturvatoimintojen noudattamista on mahdollista tukea motivoimalla henkilöstöä ja viestimällä siitä, mitkä asiat ovat organisaatiolle tärkeitä.

Asioista, jotka ovat organisaatiolle tärkeitä, muodostuu strategisia tavoitteita. Näistä johdetaan kriittisiä menestystekijöitä, joilla tarkoitetaan liiketoiminnan onnistumisen ja strategisten tavoitteiden toteutumisen kannalta keskeisiä asioita (Lönnqvist, 2002). Kujansivu et al. (2007) jakavat menestystekijät syytekijöihin ja tulostekijöihin. Syytekijät vaikuttavat jollain tavalla tulostekijöihin, jotka sitten kertovat varsinaisista liiketoiminnan tavoitteista. Menestystekijä voi myös olla samanaikaisesti syy- ja tulostekijä. Kuvassa 3.3 esitellään menestystekijöiden välisiä suhteita siten, että menestystekijä ”henkilöstön osaaminen” on otettu esimerkiksi ja pohdittu mihin se vaikuttaa. Menestystekijöiden välisiä suhteita hahmottamalla mittareita voidaan asettaa eri johtotasoille ja huomioida, miten alemman tason mittari mahdollisesti vaikuttaa ylemmän tason mittareihin.

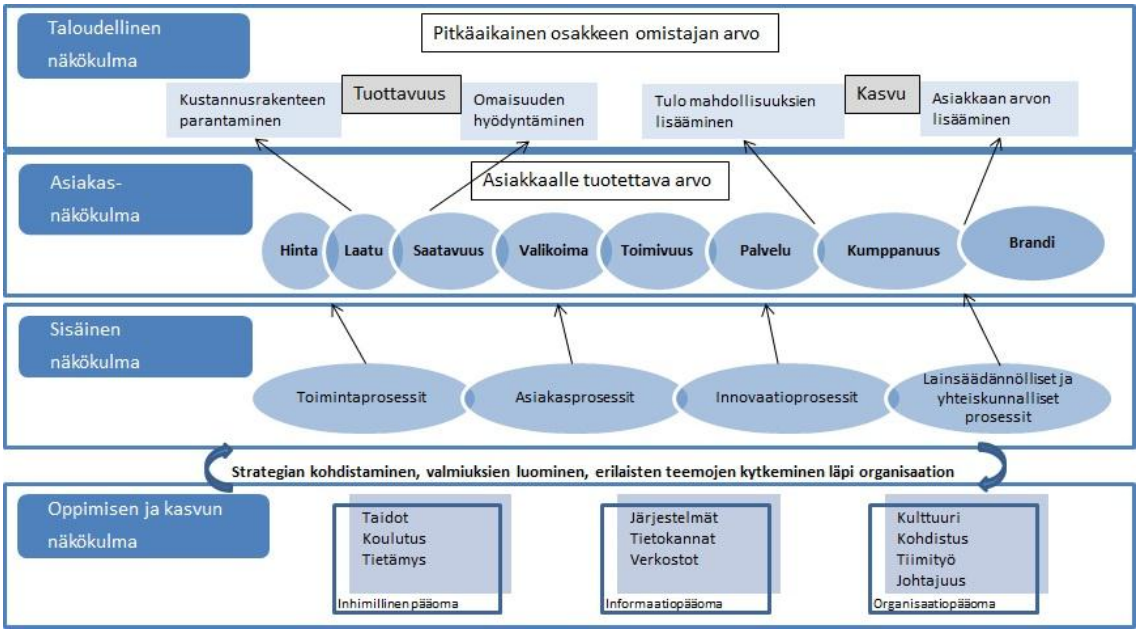


Kuva 3.3. *Menestystekijöiden väliset suhteet (Mukailtu lähteestä Kujansivu et al. 2007)*

Menestystekijät voidaan jakaa taloudellisiin ja ei-taloudellisiin tekijöihin. Taloudellisia menestystekijöitä ovat kannattavuus ja vakavaraisuus. Ei-taloudellisiksi menestystekijöiksi luetaan toimitusaika, laatu ja tuottavuus. Toisaalta menestystekijöiden voivat olla myös aineettomia, esimerkiksi osaaminen ja asiakastyytyväisyys, tai aineellisia, esimerkiksi kannattavuus, toimitusaika ja tuottavuus. (Kujansivu et al. 2007.) Näiden jaottelujen perusteella voidaan pohtia syy-seuraus suhteita ja muodostaa suorituskykymittareita. Jaottelu auttaa ymmärtämään, mistä jokin menestystekijä muodostuu ja näin ollen ymmärtämään paremmin mitä organisaatiossa kannattaa mitata osana strategista johtamista. Menestystekijät on syytä ottaa huomioon mittareita suunnitellessa ja tunnistaa, mihin toimintaan ne liittyvät. Kuvaan 3.3 tietoturvallisuuden voisi liittää ainakin osaksi toiminnan tehokkuutta ja palvelun laatua. Yleinen näkemys on, että tietoturvallisuus hidastaa organisaation toimintaa, mutta sitä tehostamalla voidaan lisätä työn kannattavuutta. Toisaalta huono tietoturvallisuus heijastuu tuotteiden ja palveluiden laatuun. Henkilöstön osaaminen ja ymmärrys tietoturvallisuudesta vaikuttaa näihin molempiin ja parantaa asiakasuskollisuutta. Seuraavassa luvussa pohditaan tarkemmin, miten tietoturvallisuus suhtautuu organisaation toimintaan perinteisestä mittaamisen näkökulmasta.

3.3 Tasapainotettu mittaristo ja tietoturvallisuuden menestystekijät

Brotby (2010 s. 79) esittelee ja arvioi tehokkaita tietoturvamittaristo vaihtoehtoja, mutta tyytyy toteamaan, että johtamisen kannalta tasapainotettu tietoturvamittaristo olisi paras vaihtoehto. Tässä näkemyksessä ei syvennytä siihen, mitkä olisivat eri osa-alueiden tärkeimmät mittarit. Jaquith (2007, s. 264-293) sen sijaan suunnittelee tietoturvamittareita tasapainotetun tuloskortin viitekehyksen mukaisesti, muttei sido niitä liiketoimintaan liittyviin tavoitteisiin. Tässä luvussa esitellään tasapainotettu mittaristo. Tasapainotettua tietoturvamittaristoa kuvaillessa esitellään tietoturvamittareita, joita aiheen kirjallisuudessa liitetään siihen. Muita kirjallisuuden tietoturvamittareita ja erilaisia jaotteluja niiden suhteen esitellään tarkemmin luvussa 4. Kuvassa 3.4 on esitelty tasapainotettu mittaristo, jossa hahmotellaan myös eri näkökulmien suhteita toisiinsa.



Kuva 3.4. *Tasapainotettu tuloskortti. (Mukailtu lähteestä Kaplan & Norton 2004, s. 72)*

Tietoturvallisuus on johdon näkökulmasta usein tukifunktio. Ylisirniö (2011, s. 209-210) mainitsee, että pelkästään lokaaleja mittauksia tekemällä ei saada esimerkiksi tukifunktioista sellaista arvoa esille, jota johto oikeasti tavoittelee. Mittaamisessa tulee pyrkiä yhdistämään strategiset tavoitteet, saatu informaatio sekä johdon ja organisaation toimenpiteet. Tasapainotettu tuloskortti esittelee strategiset tavoitteet jaoteltuna kuvan 3.4 mukaisesti neljään näkökulmaan, joihin voidaan liittää toimenpiteitä ja pohtia, miten niistä kerätään tietoa. Strategian avulla kuvataan perinteisesti, miten organisaatio tuottaa arvoa osakkeenomistajille. Esimerkiksi tietämyksen ja teknologian kaltainen aineetonpääoma ei yleensä vaikuta suoraan taloudelliseen tulokseen, vaan niiden vaikutus muodostuu syy ja seuraus –suhde ketjujen kautta. Esimerkiksi työntekijöiden koulutus voi parantaa laatua, joka lisää asiakastyytyväisyyttä, mikä lisää puolestaan asiakasuskollisuutta. Toisaalta aineeton pääoma muutetaan taloudelliseksi markkina-arvoksi sisäisten prosessien, suunnittelun, tuotannon, toimitusten ja asiakaspalvelun avulla. Sisäiset prosessit tulee siis suunnata arvon tuottamiseen asiakkaille. (Kaplan & Norton 2004, s. 51-51.) Tietoturvallisuus on osa organisaation toimintaa läpi arvoketjun, mutta tukifunktiona sen rooli jää usein kustannuseräksi. Seuraavaksi liitetään tietoturvallisuus tasapainotetun tuloskortin eri näkökulmiin.

3.3.1 Taloudellinen näkökulma

Tasapainotetun tuloskortin taloudellisessa näkökulmassa tulosmittarit pyrkivät ilmaisemaan, tukeeko organisaation strategia ja sen toteutus yrityksen taloudellisten tulosten parantamista. Taloudelliset tavoitteet liittyvät usein kannattavuuteen. Niitä mitataan esimerkiksi operatiivisella tuloksella ja sijoitetulle pääomalle saadulla tuotolla, eli tutkitaan miltä organisaatio näyttää osakkeen omistajien kannalta. Nämä mittarit kertovat yksinkertaistetun lopputuloksen siitä, kuinka paljon organisaatiot ansaitsevat ja kuluttavat. Taloudellisesta näkökulmasta organisaation tulos paranee siis tulojen kasvun ja

tuottavuuden avulla. Organisaation toiminta, esimerkiksi tietojohtaminen, uuden teknologian käyttö ja laadun parantaminen, tuottaa arvoa vain jos se lisää myyntiä tai alentavat kuluja. (Kaplan & Norton 2004, s. 58-60.) On huomioitava, että taloudelliset mittarit eivät kuvaile keinoja tai syitä, joiden mukaan tulos muodostuu. Organisaation tulos riippuu strategisten toimintojen lisäksi myös yleisemmästä taloudellisesta tilasta tai kilpailukentän nopeista muutoksista. Strategian onnistumisen vaikutusta tulokseen ei siis voida yksiselitteisesti näiden mittareiden perusteella nähdä.

Yritykset voivat kasvattaa liikevaihtoaan ja parantaa taloudellista tulostaan syventämällä asiakassuhteitaan, jolloin yritys voi myydä enemmän olemassa oleville asiakkaille. Muut vaihtoehdot ovat joko myydä uusia tuotteita tai löytää uusia asiakkaita. (Kaplan & Norton 2004, s.58.) Tietoturvallisuuden näkökulmasta tähän ei voida suoranaisesti vaikuttaa, mutta tuotteiden tietoturvaominaisuudet saattavat tuoda joillekin asiakasryhmille lisäarvoa tai parantaa työn tuottavuutta. Esimerkiksi Wiander (2007) mainitsee, että yritysten motivaationa kehittää tietoturvallisuutta on toisinaan kilpailukyvyn parantaminen ja myynnin tukeminen. Nämä asiat ovat liikevaihdon kasvattamiseen pyrkivinä toimenpiteinä. Toisin sanoen yritys pyrkii osoittamaan, että se on luotettava toimia, jonka kanssa kannatta tehdä kauppaa. Vaatimuksia tähän tulee usein asiakasnäkökulmasta. Tästä voidaan päätellä että se, miten hyvin ulkopuoliset tahot arvioivat organisaation tietoturvallisuuden, on tietoturvallisuuden menestystekijä. Tasapainotetun tuloskortin mukaisesti tämä voidaan viedä käytännön tasolle asiakasnäkökulmaa tarkkaillen, johon vastataan sisäisen toiminnan kautta.

Kaplanin & Nortonin (2004, s.58) mukaan tuottavuutta pystytään parantamaan kahdella tavalla: pienentämällä kuluja ja hyödyntämällä omaisuuttaan tehokkaammin. Tuottavuuden kannalta tietoturvallisuus liittyy taloudelliseen näkökulmaan kulujen vähentämisen kautta. On kuitenkin huomioitava, että kyseessä olevat summat eivät ole yrityksen mittakaavassa kovinkaan suuret. Jaquith (2007, s. 272) esittelee taloudelliseen näkökulmaan liittyviä tietoturvamittareita. Näitä ovat muun muassa:

- Tietojärjestelmän käyttökatkoista johtuvat kustannukset
- Tietoturvatapauksista aiheutuvat kustannukset
- Tietoturvallisuuden budjetti
- Tietoturvamenetelmien määrä
- Tietoriskien määrä

Taloudelliseen näkökulmaan liitettävät mittarit ovat usein johdolle merkityksellisimpiä, sillä kuten luvussa 2.3.1 esiteltiin, johdon tietotarpeena ovat rahamääräiset mittarit. Esimerkiksi käyttökatkoihin liittyvään mittariin voidaan koostaa useista mittareista, jotka mittaavat organisaation järjestelmien häiriöitä. Tietoturvatapahtumiin liittyvät kustannukset pystytään liittämään osaksi käyttökatkoja tai päinvastoin, jolloin saataisiin kokonaiskuva kustannuksista. Yksityiskohtaisemmat mittarit taas voisivat tukea tietoturvapäällikön työtä. Tietoturvamenetelmiä ja riskejä mittaamalla organisaatiolla on

mahdollisuus muodostaa kokonaiskuva tietoturvallisuuden tilasta ja siitä, mihin tietoturvakustannukset allokoidaan. Myös tämä nähtiin johdon tietotarpeena. Tietoturvatoiminnot pystytään liittämään asiakasnäkökulmaan seuraamalla, kuinka moni niistä vastaa johonkin asiakasvaatimukseen. Tämä mittari voisi tosin olla pikemminkin tietoturvapäällikön tietotarpeisiin sopiva. Tietoturvabudjetti on vahvasti ylimmän johdon määriteltävissä. Sen seuraaminen ja suunnittelu on tietoturvapäällikön tai tietohallintojohtajan tehtävänä.

3.3.2 Asiakasnäkökulma

Strategiakartan asiakasnäkökulmasta johtajat määrittelevät ne asiakassegmentit, joissa yritys tai sen liiketoimintayksikkö kilpailee. Näiden segmenttien osalta pyritään selvittämään miltä organisaatio näyttää asiakkaiden näkökulmasta, eli kuinka organisaatio täyttää arvolupauksensa. Arvolupaus sisältää tuote-, hinta-, palvelu-, asiakassuhde-, ja imagoyhdistelmän, joiden kautta asiakassegmenteille viestitetään miten yritys aikoo kohdella asiakkaitaan. Asiakasnäkökulman tulosmittareita tarkastellaan syy-seuraus – suhteina. Asiakkaiden tyytyväisyys takaa usein pysyviä asiakassuhteita ja mahdollistaa sekä uusien asiakkaiden saannin että isomman osuuden asiakkaan hankinnoista. (Kaplan & Norton 2004, s. 62.) Tietoturvallisuus liittyy asiakaslupaukseen usein asiakasvaatimusten kautta. Asiakkaat voivat vaatia tietynlaisia tietoturvatoimintoja yritykseltä, esimerkiksi ISO/IEC 27001 standardin mukaista toimintaa. (Wiander 2007.) Tällaiset vaatimusten kautta yritys voi ennakoiden tavoitella hyvää mainetta ja auttaa yritystä ymmärtämään miten sen tietoturvallisuus vaikuttaa ulkopuolisiin toimijoihin (Jaquith 2007). Asiakasvaatimusten ja muiden vaatimusten täyttäminen on tietoturvallisuutta parantava asia, eli tietoturvallisuuden menestystekijänä (Kwon & Johnson 2012).

Kaplan & Norton (2004) eivät suoranaisesti liitä asiakkaan vaatimuksia asiakasnäkökulmaan, mutta he puhuvat asiakastavoitteista, joista ilmenee niiden taustalla olevat vaatimukset. Asiakastavoitteita on tässä yhteydessä kaikki kolmansien osapuolien asettamat tietoturvavaatimukset. Organisaation tuotteita ja palveluja voidaan tarkastella laadun, saatavuuden ja toimivuuden näkökulmasta, joiden tulee täyttää asiakkaan odotukset tavoitteiden täyttymiseksi. Näihin tavoitteisiin vaikuttaa myös tietoturvallisuus. Esimerkiksi saatavuus on yksi tekijä, jonka kautta tietoturvallisuus määritellään, kuten luvussa 2.2 esiteltiin. Tästä voidaan päätellä, että kaikki organisaation tietoon liittyvät saatavuus-, laatu- ja toimivuusongelmat vaikuttavat asiakastavoitteiden täyttymiseen. Kuvassa 3.4 esitellään palvelu, kumppanuus ja brandi. Nämä imagoon ja asiakassuhteeseen liittyvät asiat ovat sidoksissa tietoturvallisuuteen. Wianderin (2007) esittelemässä tutkimuksesta osa yrityksistä perusteli tietoturvallisuuden kehittämistä paremman julkisuuskuvan kautta. Myös Jaquith (2007, s. 278) mainitsee hyvän maineen tärkeänä tietoturvavaatimuksena ja lisää elektronisen kaupankäynnin hyödyntämisen maksimoinnin tärkeäksi tavoitteeksi asiakasnäkökulmaan. Asiakasnäkökulmaa kuvailevia tietoturvamittareita ovat Jaquithin (2007, s. 279-280) mukaan esimerkiksi:

- Tietoturvallisuuteen liittyvät asiakasmenetykset ja voitetut asiakkuudet
- Asiakkaiden tekemien tietoturva-auditointien läpäisyprosentti
- Kolmansiin osapuoliin liittyvien sopimusten osuus, joissa on huomioitu tietoturvavaatimukset
- Kolmansien osapuolien tietoturvallisuuden katselmukset
- Kolmansiin osapuoliin liittyvät tietoturvatapahtuma

Asiakasmenetysten ja voitettujen asiakkuuksien määrää saattaa olla haastava mitata, jos asiakassuhde ei ole läheinen ja syitä asiakkaan päätöksiin ei pystytä erittelemään. Mikäli tällainen mittari on mahdollista kehittää, voisi sen perusteella arvioida tietoturvallisuuden resursseja ja asiakkaiden näkemystä organisaation tietoturvallisuuden tilasta. Jaquithin (2007, s. 279) esittelemä tietoturva-auditointien läpäisyprosentti kuvailee yhtälailla asiakkaiden näkökulmaa, mutta siihen pystytään liittämään yleisimpiä syitä sille, miksei auditointia läpäistä. Tämän avulla asiakasnäkökulman kautta voidaan kehittää sisäistä toimintaa. Kolmansien osapuolten katselmusten ja vaatimusten avulla voidaan pohtia organisaation ulkopuolisten tahojen vaikutusta organisaation tietoturvallisuuteen. Kolmansiin osapuoliin liittyvät tietoturvatapahtumat voivat muodostua liiketoimintaan liittyviksi riskeiksi ja niillä on usein taloudellisia vaikutuksia, jolloin ne voi olla tarpeellista raportoida johtotasolle.

3.3.3 Sisäinen näkökulma

Asiakasnäkökulman tavoitteet kuvastavat strategiaa ja arvolupausta, joiden menestyksekästä toteutusta kuvastavat taloudellisen näkökulman tavoitteet. Kun organisaatio on hahmottanut taloudelliset ja asiakkaisiin liittyvät tavoitteet, sisäisen näkökulman avulla ilmaistaan kuinka strategiaa toteutetaan. (Kaplan & Norton 2004, s. 64-65.) Kuten luvussa 2.4 kuvailtiin, tietoturvallisuuden toteutukseen liittyvät menetelmät johdetaan ensin strategiasta, jonka jälkeen asetetaan siihen liittyviä tavoitteita ja periaatteita, joiden mukaan tietoturvallisuutta toteutetaan. Toisaalta tietoturvallisuutta voidaan tarkastella osana sisäisiä toimintoja. Joissakin tapauksissa tietoturvallisuus voi kokonaisuudessaan olla sisäinen osa-alue, jossa organisaation tulee olla parhaimmillaan.

Kuvassa 3.4 esitetään, kuinka sisäinen näkökulma jaetaan toimintaprosesseihin, asiakasprosesseihin, innovaatioprosesseihin ja lainsäädännöllisiin seikkoihin. Näihin prosesseihin kytketään asiakastavoitteet, eli pyritään parantamaan toimitusketjua, tuotetta ja palvelua, asiakassuhteita sekä imagoa. Tietoturvallisuuden avulla yritystä suojellaan haitallisilta asioilta, eli esimerkiksi toimitaan vain luotettujen toimijoiden kanssa ja vähennetään todennäköisyyttä tietomurroille ja muille tietoturvatapahtumille. Toisaalta sisäisestä näkökulmasta tietoturvallisuus takaa pääsyn resursseihin, kun niitä tarvitaan, eli maksimoi tietoon liittyvien palveluiden saatavuuden. Usein tietoturvallisuus kuitenkin nähdään sisäistä toimintaa ja toiminnan kehittymistä hidastavana tekijänä. (Jaquith 2007, s. 282-283.)

Wianderin (2007) mukaan tietoturvallisuutta kehitetään toissijaisesti puhtaasti sisäisen toiminnan näkökulmasta, sillä usein tavoitteet tulevat asiakasvaatimusten tai muiden kolmansien osapuolten vaatimusten kautta. Tämä näkemys sopii myös strategiakarttojen ajattelutapaan. Jaquithin (2007, s.282-283) esittelemiin tietoturvallisuuden sisäisiin asioihin liittyen Wiander (2007) mainitsee laadun parantamisen, parhaiden käytäntöjen implementoinnin ja paremmin hahmotettavan tietoturvaviitekehyksen sekä huomioivan riskienhallinnan näkökulman. Näillä tekijöillä pyritään suojaamaan sisäistä toimintaa ja ylläpitämään hyvää saatavuutta. Laadun parantamisen voi nähdä kahdella tavalla: tietoturvallisuuden laadun parantaminen ja yleisesti laadun parantaminen paremman tietoturvallisuuden ansiosta. Tietoturvallisuuden laadun parantamisen tarkoittaa esimerkiksi tietoturvallisuuden kehittämistä sujuvaksi osaksi liiketoimintaa, jottei sen koettaisi hidastavan sisäistä toimintaa. Esimerkiksi tietoturvallisuudesta johtuvan byrokratian vähentäminen voisi olla tällainen tavoite. Parempi laatu liittyy innovaatioprosesseihin, joissa tietoturvallisuus pystytään huomioimaan alusta alkaen ja näin tuoda markkinoilla tietoturvallisia tuotteita ja palveluja. Näin tietoturvallisuus vaikuttaisi positiivisesti yrityksen imagoon.

Koska sisäisen toiminnan näkökulmasta tärkein tehtävä on toteuttaa sellaisia prosesseja, jotka tuottavat asiakkaalle arvoa, voidaan tietoturvallisuuden tehtävänä pitää tämän arvon tuoton varmistamista. Esimerkiksi asiakkaaseen liittyvien tietojen säilyttäminen huolellisesti ja tietoturvallinen kommunikointi asiakkaan kanssa ovat tärkeitä asioita. Tietoturvaresurssien määrä, kuten erilaista turvallisuutta lisäävät tietotekniset sovellukset osana prosesseja, korreloi tietoturvallisuuden tasoon. Toisin sanoen tietoturvallisuuden menestystekijänä sisäisestä näkökulmasta on, kuinka kattavasti eri järjestelmissä on huomioitu tietoturvallisuus. Sisäisen toiminnan menestystekijöitä ovat lisäksi tietoturvapolitiikan mukaisen toiminnan ja tietoturvallisuuden arviointien tiheyden. (Kwon & Johnson 2012.) Jaquith (2007, s. 285-286) esittelee muun muassa seuraavat tietoturvamittarit liittyen sisäiseen näkökulmaan:

- Aika, joka kuluu siihen että kaikki järjestelmät on päivitetty
- Vaatimusten mukaisten järjestelmien osuus
- Osuus varmenteista, joita säilytetään erillisessä ympäristössä
- Niiden varmuuskopioiden osuus, joita säilytetään erillään
- Tietoturvatapahtumien kustannukset ja niiden aiheuttama järjestelmien alhaalla oloaika

Sisäisen toiminnan mittarit ovat tietoturvapäällikön ja jossain määrin tietohallintojohtajan tietotarpeita täyttäviä. Järjestelmien päivitysaika ja vaatimusten mukaiset järjestelmät kuvailevat sisäistä tietoturvatoimintaa kokonaisuudessaan, kun taas varmenteiden ja varmuuskopioiden säilytystä kuvaavat mittarit on esimerkkejä vahvasti teknisestä ja käytännön läheisistä mittareista. Tämän ja vastaavien mittareiden avulla voidaan viestiä järjestelmien ylläpitäjille tietoturvatavoitteita ja valvoa, että organisaation toiminta on

asiakasvaatimusten mukaista. Tietoturvapäällikön mittaristo voisi olla kokoelma näistä. Jaquith (2007, s. 285-286) esittelee tietoturvatapahtumien kustannukset ja järjestelmien häiriöt myös sisäisen toiminnan osana. Sisäisen toiminnan näkökulmasta näillä mittareilla mitataan yksityiskohtaisemmin sitä, mistä kulut muodostuvat ja ovatko ne kasvaneet tai vähentyneet.

3.3.4 Oppiminen ja kasvu

Tasapainotetun tuloskortin neljäs näkökulma, oppiminen ja kasvu, kuvaa organisaation aineetonta pääomaa ja sen roolia strategiassa. Usein aineeton pääoma jaetaan kolmeen luokkaan, inhimilliseen pääomaan, informaatiopääomaan ja organisaatiopääomaan. Nämä kuvailevat käytettävissä olevia, strategian toteutusta tukevia henkilöstön tietoja ja taitoja, organisaation tietojärjestelmiä ja muita teknisiä arkkitehtuureja sekä organisaation kykyä käynnistää strategian toteuttamiseen tarvittava muutosprosessi. Oppimisen ja kasvun näkökulmasta organisaation tulisi keskittyä tukemaan erityisominaisuuksia, joita tärkeät sisäiset prosessit edellyttävät. (Kaplan & Norton 2004, s. 73.) Keskittämällä osaamistaan niihin asioihin, joissa organisaation tulee sisäisten toimintojen näkökulmasta olla parhaimmillaan, auttaa organisaatiota ymmärtämään ja palvelemaan asiakkaitaan paremmin. Tämä taas johtaa kasvuun ja kannattavuuden parantamiseen.

Tietoturvallisuus on harvoin sisäinen tekijä, joka henkilöstön tulee osata täydellisesti. Muun muassa tästä syystä oppimisen ja kasvun näkökulmaa ei tule painottaa liikaa tietoturvallisuuden kannalta. Jaquith (2007, s. 288) painottaa, että tästä näkökulmasta henkilöstön vastuuta pitäisi kasvattaa tietoturvallisuudesta siten, että se ei ole pelkästään tietoturvallisuusyksikön vastuulla. Tällä tavoin turvallisuutta on mahdollista yhdistää enemmän liiketoimintaprosesseihin. Lisäksi liiketoimintaan liittyvässä päätöksenteossa huomioitaisiin tietoturvallisuus, mikäli päätöksentekijällä olisi vastuu tietoturvallisuuden toteutumisesta. Tämän tueksi tulee varmistaa, että tietoturvallisuudesta on riittävä osaaminen ja kehittää tietojärjestelmien tietoturvallisuutta siten, että se ei hidasta työntekoa. Näin ollen tietoturvayksikkö voisi keskittyä enemmän uusien uhkien tunnistamiseen ja ennakoivampaan työhön, jolloin tietoturvallisuudesta muodostuisi luonnollisempi osa organisaation toimintaa. (Jaquith 2007, s. 288-292) Esimerkkimittareita oppimisen ja kasvun näkökulmaan ovat:

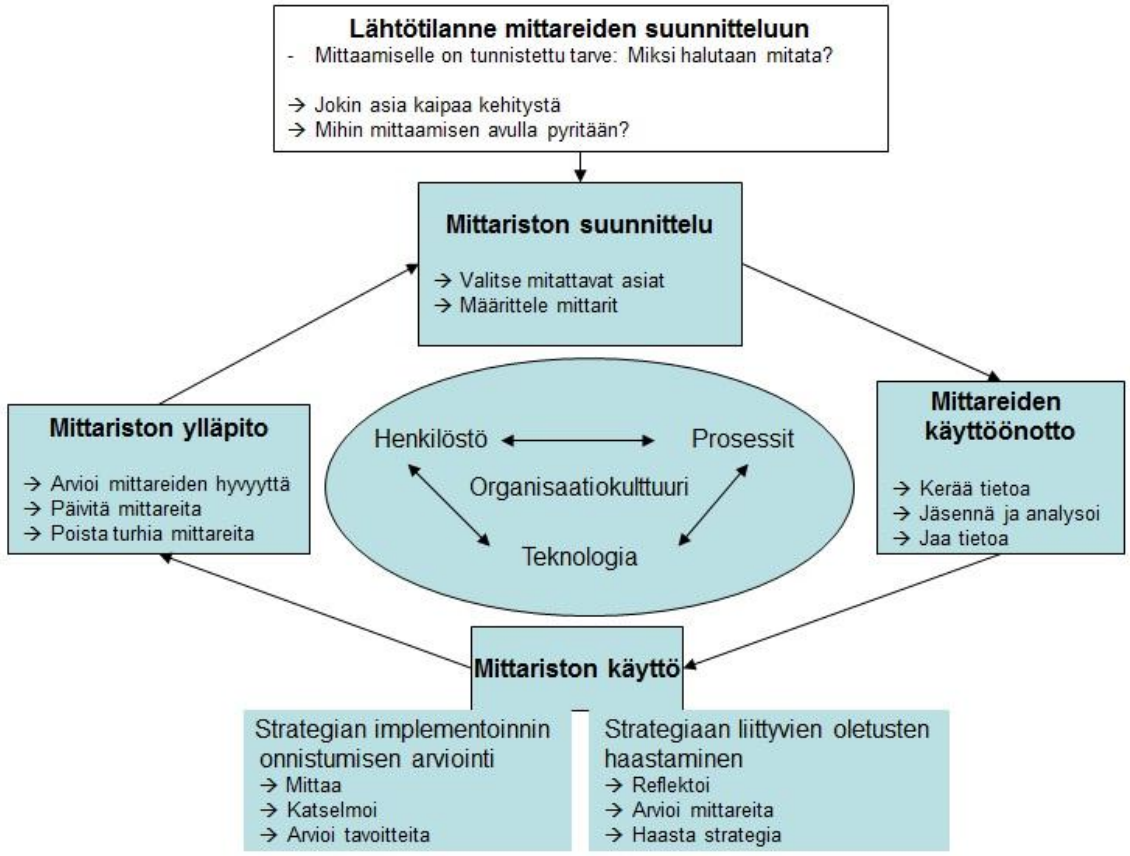
- Osuus uusista työntekijöistä, jotka saavat tietoturvakoulutuksen
- Järjestelmien määrä, joiden suunnittelussa on huomioitu tietoturvallisuus alusta saakka
- Osuus niistä työrooleista, joiden osalta on arvioitu niihin liittyvät tietoturvavaatimukset

Lisäksi Jaquith (2007, s. 292) esittelee useita mittareita, joilla mitataan tietoturvatietoisuuden tasoa, tietoturvasertifikaatin omaavia henkilöiden määrää organisaatiossa, tietoturvasta jollain tavalla vastuussa olevien osuutta kaikista työntekijöistä ja niin edelleen.

Kwon & Johnson (2012) esittelevät tietoturvallisuuden menestystekijöiksi tietoturvatietoisuuden ja tietoturvallisuuden huomioimisen uusien työntekijöiden rekrytoinnin ohella. Osaamisen tasoa kuvailevia mittareita on suhteellisen helppo toteuttaa, mutta niitä suunnitellessa tulee huomioida, mitä niiden avulla oikeasti voidaan tietää organisaation toiminnasta. Käytännössä yksi vaihtoehto voisi olla kouluttaa sellaisia asioita, jotka koetaan sisäisesti tärkeiksi ja mittaamisen avulla motivoida henkilöstöä osallistumaan näihin koulutuksiin.

3.4 Mittariston suunnittelu

Mittarin kehitysprosessi muodostuu neljästä päävaiheesta, joista ensimmäisessä valitaan mitä mitataan ja millä mittareilla. Tämän jälkeen mittaristo otetaan käyttöön, jolloin asianomaiset henkilöt koulutetaan mittariston käyttöön. Mittaristoa tulee myös analysoida ja ylläpitää tarpeen mukaan, mikä antaa tietämystä mittariston suunnittelulle. Mittariston ylläpitoa tulee tehdä strategian tai prosessien muutosten yhteydessä. Mittaamisen ohessa pitää huomioida sen avaintekijät, eli henkilöstö, jota mittaus koskee; prosessit, joita mittariston käyttöön liittyy; infrastruktuuri, joka toimii mittariston taustalla ja organisaatiokulttuurin vaikutukset mittaamiseen. (Neely et al. 2000.) Bourne et al. (2000) esittelevät suorituskyvyn mittariston kehittämisen ensimmäiset vaiheet samoin kuin Neely et al. (2000) mutta täsmentävät mittariston käyttöä. Mittaristoa voidaan käyttää strategian implementoinnin tukena tai haastamaan strategiaan liittyviä oletamuksia. Kun mittaristoa käytetään strategian implementointiin, mittaustuloksia verrataan asetettuihin tavoitteisiin ja reagoidaan tulosten mukaisesti. Strategiaa haastettaessa tuloksien avulla pohditaan, tekeekö organisaatio oikeita asioita. Kujansivu et al. (2007, s. 166-167) taas huomauttavat, että kehitysprosessi on usein iteratiivinen, eli että se ei etene suoraan vaiheesta toiseen. Neelyn et al. (2000) ja Bournen et al. (2000) malleissa ylläpito voidaan nähdä iteroivana kohtana prosessia, koska siihen voidaan palata kaikista muista vaiheista. Kuvassa 3.5 on esitetty suorituskyvyn mittaamisen päävaiheet ja avaintekijät, jotka tulee huomioida osana mittareiden kehittämistä.



Kuva 3.5. *Suorituskyvyn mittaamisen päävaiheet. (Mukailtu lähteistä Bourne et al. 2000; Neely et al. 2000; Kujansivu et al. 2007, s. 166; Ylisirniö 2011, s. 215)*

Mittariston suunnitteluvaiheessa tunnistetaan asiakkaisiin ja sidosryhmiin liittyviä tarpeita. Tarpeita etsitään suoraan strategisiin tavoitteisiin liittyen siten, että liiketoimintaa analysoidaan eri näkökulmista ja pohditaan mitkä asiat siihen vaikuttavat suhteessa tavoitteisiin. Tavoitteiden tunnistaminen ja asettaminen on tärkeää, jotta voidaan määritellä toiminnot jotka niiden toteutumista tukevat. Suunnitteluvaiheessa johdon on otettava vastuuta mittariston kehittämisestä, jotta mittaristoon liitettävät menestystekijät ja tavoitteet sidotaan mahdollisimman läheisesti liiketoimintaan. (Bourne et al. 2000.) Myös Lönnqvist et al. (2006, s. 103) toteavat, että mittariston suunnittelun perustana on organisaation strategia, jonka perusteella tunnistetaan menestystekijät ja asetetaan mittauksen tavoitteet. Johdon lisäksi mittariston suunnitteluun on otettava mukaan henkilöstö, jotta mittariston käyttöönotto helpottuu ja tavoitteista muodostuu yhteisiä. Suunnitteluvaiheessa on huomioitava teknologian asettamat rajoitteet ja määritettävä sen käyttöperiaatteet.

Bournen et al. (2000) mukaan mittariston suunnitteluvaihetta voidaan toteuttaa työpajoissa, joihin osallistuu johtoryhmä. Suunnitteluvaiheessa suoritetaan kokonaisanalyysi, jonka Ylisirniö (2011, s. 215) mainitsee antavan tarvittavat lähtötiedot strategian mittaamisen käyttöönotolle ja prosessille. Kokonaisanalyysissä organisaatiota tarkastellaan nykyisen strategian ja järjestelmien näkökulmasta. Strategiaan liittyviä kokonaisuuksia

ovat sen sisältöteemat, nykyisen mittaamisen arviointi ja strategiaprosessi. Järjestelmiin liittyviä elementtejä ovat johtamiseen ja työnohjaamiseen liittyvät järjestelmät. Lisäksi organisaation rakennetta ja niihin kuuluvia verkostoja tulee tarkastella, jotta löydetään strategiaan vaikuttavia tekijöitä. (Ylisirniö 2011, s. 215-216.) Brotby (2009, s. 63) mainitsee samankaltaiset asiat osana tietoturvamittareiden suunnittelua, mutta painottaa myös, että on tärkeää pohtia kenelle mittarit osoitetaan. Osana kokonaisanalyysiä tulee selvittää ainakin (Ylisirniö 2011) mukaan seuraavat asiat:

- Mihin mittaaminen kohdistuu?
- Mitä mittaamisella tavoitellaan?
- Mitä mittausjärjestelmä sisältää?
- Mitä mittausmenetelmiä on jo käytössä?
- Millaiset edellytykset strategian mittaamiselle organisaatiossa on?

Tämän tutkimuksen osalta mittaaminen kohdistuu tietoturvallisuuteen ja mittaamisella tavoitellaan mahdollisimman kuvaavaa esitystä tietoturvallisuuden tilasta. Tämä on kuitenkin liian laaja kysymys, johon voidaan vastata tunnistamalla yksityiskohtaisempia kohteita. Mittaaminen voi Ylisirniön (2011, s. 215) mukaan kohdistua toiminnan kattavuuden ja painopiste alueiden tarkasteluun. Tämän jälkeen voidaan pohtia kyvykkyyksiä ja osaamista näillä alueilla. Tasapainotetun tuloskortin käyttäminen on yksi esimerkki pohtia liiketoiminnan mittaamista eri näkökulmista. Osana toiminnan arviointia sen esteet ja mahdollisuudet voivat olla mittaamisen kohteina. Tietoturvallisuuden näkökulmasta toiminta voi tarkoittaa tietoturvallisuuden hallinnointiin liittyviä toimintoja, tietoturvamenetelmien toimivuutta tai tietoturvaprosesseja (ISO/IEC 27004).

Kokonaisanalyysin tavoitteena on loppujen lopuksi tavoitteena löytää menestystekijöitä, joita halutaan johtaa ja joista halutaan informaatiota (Kujansivu et al. 2007, s. 168). Näitä menestystekijöitä ja niiden johtamista suorituskyvyn mittareiksi pohdittiin edellisessä luvussa. Mittareiden suunnitteluvaiheessa päädytään määrittelemään tällaisia mittareita, mutta olennainen osa suunnittelua on tunnistaa, miten mittareita tullaan käyttämään ja miten menestystekijöistä saadaan tietää juuri oikeita asioita. Menestystekijöitä voidaan mitata joko suorilla, välillisillä, objektiivisella tai subjektiivisilla mittareilla. Suorilla mittareilla mitataan suoraan sitä asiaa, josta halutaan tietoa. Koska tämä ei aina ole käytännössä mahdollista, menestystekijästä on mahdollista saada tietoa mittaamalla jotain asiaa, joka on siihen läheisesti sidoksissa ja jonka tiedetään kertovan siitä jotain. Esimerkiksi osaamisen mittaamista pystytään tekemään välillisesti mittaamalla koulutuksen määrää. Tosin on relevanttia pohtia, kuvaako koulutuksen määrä osaamista, mutta mittarin voidaan olettaa aktivoivan työntekijöitä osallistumaan koulutuksiin. (Kujansivu et al. 2007, s. 168-169)

Objektiiviset mittarit antavat nimensä mukaisesti objektiivisen kuvan mittauksen kohteesta ja ne soveltuvat hyvin konkreettisten toimintojen mittaamiseen. Objektiiviset mittarit antavat tarkan arvon mittauskohteesta, josta syystä niitä pidetään hyvinä ja luotet-

tavina. Tällaisia mittareita ovat esimerkiksi liikevaihto ja toimitusaika. Subjektiiviset mittarit taas antavat tuloksen, joka perustuu mielipiteisiin tai arvoihin. Näitä mielipiteitä kerätään kyselyillä tai haastatteluilla, joiden tuloksista lasketaan indeksejä ja tunnuslukuja. Tyypillisesti asiakastyytyväisyyttä ja henkilöstötyytyväisyyttä mitataan subjektiivisilla mittareilla. Subjektiivinen mittari voidaan suunnitella siten, että sen avulla huomioidaan kaikki mittaamisen kohteeseen liittyvät osa-alueet. Näin subjektiiviset mittarit ovat kattavia, mutta niiden tarkkuus ei ole yhtä hyvä kuin objektiivisissa mittareissa. (Kujansivu et al. s. 169-170)

Mittarien suunnitteluun on hankala antaa selkeää ohjeistusta, sillä mittausprosessi riippuu mitattavasta tekijästä, mittaustilanteesta ja käytössä olevista resursseista. Kun menestystekijä jota halutaan mitata on tunnistettu, voidaan mittauksen toteutusta kartoittaa seuraavilla Kujansivun et al. (2007, s. 170-172) esittelemillä apukysymyksillä:

- Onko menestystekijälle olemassa olevaa mittaria? Jos on, miten se toimii?
- Kerätäänkö mitattavaan asiaan liittyen tietoa, jota voisi hyödyntää mittarin suunnittelussa?
- Voidaanko suunnitella jokin menettelytapa, jolla menestystekijästä saadaan tietoa?
- Voidaanko tunnistaa jokin välillinen tekijä, joka kuvailee myös varsinaisen johtamisen kohteen kehittymistä?

Kun mittarin suunnitteluvaihe lähestyy loppua, tulee sen hyvyyttä arvioida validiteetin ja reliabiliteetin kautta. Validiteetti kuvaa sitä, kuinka hyvin mittari pystyy mittaamaan juuri sitä menestystekijää, josta halutaan saada tietoa. Reliabiliteetti taas kuvaa mahdollisuutta sille, että mittaustuloksessa on satunnaisvirhettä. (Kujansivu et al. 2007, s. 162.) Toisin sanoen mittauksen reliabiliteetti on korkea, mikäli mittauksia toistettaessa saadaan samoja lopputuloksia. Tietoturvallisuuden tilan mittaamisen suunnittelun kannalta validiteetti ja reliabiliteetti ovat jokseenkin ongelmallisia, sillä mittauskohteiden määritteleminen on hankalaa. Tietoturvallisuuden näkökulmasta mittareita on tunnistettu kirjallisuudessa jonkin verran. Organisaatiossa kerätään tietoturvallisuuteen liittyvää tietoa, mutta ongelmana on usein se, että tietoa kerätään vain teknisestä näkökulmasta ja suppealta alueelta sellaisia asioita, joita on helppo mitata. Sen sijaan hyviä keinoja kuvailla ja arvioida koko tietoturvallisuuden tilaa ei ole pystytty muodostamaan. (Jansen 2009)

Tietoturvamittareita suunnitellessa tulee Lippmannin et al. (2012) mukaan huomioida kolme asiaa. Ensinnäkin mittareiden tulee olla helposti ymmärrettäviä ja riittävän käytännön läheisiä, jotta ne pystytään toteuttamaan. Toisekseen jokaisen mittarin pitää arvioida täsmällisesti jotain riskiä, jonka organisaatio on tunnistanut. Kolmanneksi mittareiden tulee tukea käytäntöjä, joilla riskejä hallitaan. Lippmann et al. (2012) huomioivat mittarit vahvasti luvussa 2.5 esitellyn PDCA-mallin osaksi tukemaan toiminnan tarkastamista ja toimintaan ryhtymistä. Brotby (2009, s. 63) huomioi, että trendejä kuvailevat mittarit ovat luotettavimpia mittareita kuvailemaan tietoturvallisuutta, sillä niiden avulla

voidaan varmuudella nähdä mikä tietoturvallisuuden tila on ollut mittaushetkellä. Tähän liittyen Jaquithin (2007, s.23) mukaan mittareiden tulee olla yhdenmukaisesti mitattuja. Jotta lopputulos olisi helposti ymmärrettävä ja käytäntöön viety, tulee mittausten olla tehty samalla tavalla. Myös trendien muodostaminen on mahdotonta, jollei mittaukset ole tehty yhdenmukaisesti.

Jaquithin (2007, s. 23-24) mukaan tietoturvamittareiden tulee olla halpoja kerätä ja niiden tulisi verrata tilannetta aina johonkin tavoitteeseen. Nämä hyvän mittarin ominaisuudet tulisi liittää kokonaisanalyysin tuloksiin, jotta mittareiden käyttöönotto vaihe olisi helpompi toteuttaa. Viimeisenä testinä suunnittelu vaiheeseen sopii hyvin Jaquithin (2007, s. 25, 27) esittelemä ”So what?”-testi, jonka mittarin on läpäistävä, ennen kuin sitä kannattaa käyttää. Tässä testissä selvitetään, onko mittari relevantti kohdeyleisölleen. Testissä pohditaan yksinkertaisesti sitä, miten johto reagoi mittariin, kun se heille esitellään. Mikäli mittari aiheuttaa olan kohautuksen, voidaan päätellä että sen suunnittelussa on epäonnistuttu. Seuraavassa luvussa esitellään, mitä tietoturvamittari tarkoittaa ja mitä erityispiirteitä tietoturvallisuuden mittaamiseen liittyy.

4 TIETOTURVALLISUUDEN MITTAAMISEN NYKYTILA

Tietoturvamittareille ei ole vakiintunutta ja yleisesti käytössä olevaa määritelmää. Usein kuitenkin puhutaan tietoturvallisuuden suorituskyvyn mittaamisesta, jossa tarkastellaan organisaation tietoturvallisuuden tehokkuutta ja vaikuttavuutta (mm. Savola 2007; Jansen 2009; Brotby 2009, s. 22; Juneja et al. 2011; Savola et al. 2012). Tietoturvamittareita on kuitenkin paljon erityyppisiä ja eri tietoturvallisuuden osa-alueisiin liittyviä. Tässä luvussa esitellään, mitä tietoturvallisuuden mittaamisella tarkoitetaan. Tämän jälkeen esitellään luokituksia, joihin mittareita voidaan liittää. Luvussa paneudutaan myös tietoturvallisuuden mittaamisen haasteisiin ja siihen, miten niitä voidaan ottaa käyttöön osaksi organisaation toimintaa.

4.1 Tietoturvallisuuden suorituskyvyn mittaaminen

Tietoturvamittari tarkoittaa tietoturvallisuuden tehokkuudesta ja vaikuttavuudesta kerätyn tiedon tulkintaa ja turvallisuuden tasosta kertovia indikaattoreita (Savola et al. 2012). Brotbyn (2009) mukaan tietoturvamittari kuvaa tietoturvallisuuden tason suhteessa määriteltyyn tarkistuspisteeseen ja ohjaa tietoturvaa parantavien toimenpiteiden valinnassa. Myös Savola (2010) toteaa hyvin suunnitellun tietoturvamittarin tarjoavan uskottavaa ja riittävää tietoa tietoturvallisuuden tasosta ja suorituskyvystä päätöksenteon tueksi. Standardi ISO/IEC 27004 määrittelee tietoturvan mittaamisen tarkoittavan tietoturvallisuuden hallintajärjestelmän ja tietoturvan kontrolloinnin tehokkuudesta tietoa antavaa prosessia, jossa käytetään tiettyä metodia, laskentaa, analyyttistä mallia ja kriteerejä päätöksenteolle. Tietoturvamittari voidaankin ymmärtää hyvin samalla tavalla kuin mittarit yleisesti, kunhan ymmärretään mitä tietoturvallisuudella tarkoitetaan. Suorituskyvyn mittaamisen näkökulmasta Brotbyn ja Savolan mainitsema tietoturvallisuuden taso jaotellaan vielä kuvaavammin tietoturvallisuuden tehokkuuteen ja vaikuttavuuteen. Suorituskyvyn mittaamisen keinot voisivatkin olla sopivia tietoturvallisuuden hallinnollisen tason mittaamiseen. Tämä voidaan hahmottaa edellä esitettyjen määritelmien perusteella. Kirjallisuudessa tietoturvamittarit esitellään muun muassa tehokkuuden, vaikuttavuuden ja oikeellisuuden näkökulmasta, mutta siinä ei puhuta suoranaisesti tietoturvallisuuden suorituskyvyn mittaamisesta. (Savola 2007; Jansen 2009; Juneja et al. 2011).

Tietoturvallisuuden oikeellisuudella tarkoitetaan sitä, että tietoturvamenetelmät on implementoitu oikein ja niiden komponentit, rajapinnat ja datan prosessointi vastaa turval-

lisuusvaatimuksia (Savola 2007; Jansen 2009). Oikeellisuutta arvioidaan Jansenin (2009) mukaan tutkimalla, toimiiko tietoturvamenetelmä oikein sellaisissa olosuhteissa kuin sen on tarkoitettu. Tehokkuus tietoturvallisuuden näkökulmasta tarkoittaa, että kaikki tarkoituksenmukaiset toimintaympäristöt täyttävät turvallisuusvaatimukset ja odotukset niiden turvallisuudesta voidaan täyttää. Tehokkuuteen kuuluu myös se, että toimintaympäristöt eivät salli muunlaista toimintaa, kuin niiden kuuluu sallia. (Savola 2007; Juneja et al. 2011.) Jansen (2009) painottaa, että tehokkuus kuvastaa kuinka tietoturvallisuutta lisäävät menetelmät sopivat yhteen eri toimintaympäristöissä. Näiden menetelmien, esimerkiksi vakuutusten, teknisten suojausten tai testauksen, kautta toimintaympäristön riskejä voidaan pienentää, välttää tai hyväksyä (Savola et al. 2012). Tämän tarkoittaa sitä, onko organisaation eri osat riittävän tehokkaasti suojattu tai vakuutettu. Eri osien suojaamisessa tulee lisäksi huomioida, ettei yhteen yksikköön murtautumalla pääsee käsiksi myös muiden yksiköiden tietoihin. Tietoturvallisuuden vaikuttavuus taas osoittaa, kuinka asianmukaisesti tietoturvallisuuden tavoiteltu laatu on saavutettu resurssien, ajan ja kustannusten näkökulmasta. (Savola 2007.) Savolan (2007) ja Jansenin (2009) näkemykset sopivat luvussa 3.1 esiteltyyn suorituskyvyn tehokkuuden ja vaikuttavuuden mittaamiseen kohtalaisen hyvin. Neelyn et al. (1995) näkemys siitä, että vaikuttavuudella tarkoitetaan asiakastarpeiden täyttymistä mahdollisimman kattavasti, voisi tietoturvallisuuden näkökulmasta tarkoittaa yleisesti vaatimustenmukaisuutta.

Brotbyn (2009, s. 22-23) mukaan tietoturvallisuuden suorituskykyä osoittavat mittarit sopivat johtamisen näkökulmasta parhaiten osoittamaan tärkeimpien prosessien tai menetelmien toimivuutta. Mittaamisen tavoitteena on, että mittarit kuvailevat sitä kohtaa prosessissa, josta saadaan mahdollisimman aikaisin viitteitä mahdollisesta virheestä ja sen seurauksista. Tietoturvallisuuden hallinnoinnin näkökulmasta tällainen mittari on relevantti, mikäli mitattava prosessi on kriittinen organisaation toiminnalle ja mittarin yhteys tietoturvatapahtuman seurauksiin ymmärretään. Useat tietoturvallisuuden mittaamiseen käytettävät mittarit, kuten havaittujen haittaohjelmien määrä, palomuurin estämät mahdolliset hyökkäykset ja tietoverkon käyttöaste, eivät kuitenkaan täytyä hallinnollisen mittarin kriteerejä. Nämä ovat esimerkkejä hyvistä tietoturvamittareista, joiden käyttäjinä ovat esimerkiksi järjestelmien ylläpitäjät. Mittarin tulosten perusteella voidaan ryhtyä selvittämään syitä muutoksille mittauksen kohteissa. Esimerkkejä teknisistä tietoturvan suorituskyvyn mittareista, jotka Brotbyn (2009, s. 24) mukaan tarjoavat tietoturvallisuuden hallinnoinnin kannalta tärkeää tietoa ovat:

- Käyttökatkoihin kulunut aika
- Palvelutasosopimusten noudattaminen
- Aika joka kuluu häiriöihin reagoimiseen ja niistä toipumiseen
- Aika, joka kuluu haavoittuvuuksien havaitsemisesta toteutettuihin korjaustoimenpiteisiin

Muita suorituskykyyn liittyviä hallinnoinnin kannalta tärkeitä mittareita ovat esimerkiksi:

- Tietoturvatoimintojen vaikuttavuus
- Tietoturvatoiminnoissa havaitut virheet
- Tietoturvallisuuteen liittyvät kustannukset

Brotbyn (2009, s. 25) esittelemät ei-tekniset suorituskykymittarit painottuvat kustannusten mittaamiseen ja vaikuttavuuteen. Lisäksi mittarien yhteydessä mainitaan ”suorituskykyindikaattorit” mittaamisen kohteena. Brotby ei kuitenkaan kerro, mitä nämä ei-tekniset suorituskykyindikaattorit voisivat olla. Jaquithin (2007, s. 10) mukaan tietoturvallisuuden suorituskykyä indikoivien tekijöiden tulisi osoittaa, kuinka hyvässä kunnossa organisaation tietoturvatoiminnot ovat. Liiketoiminnan johtamisen näkökulmasta tämä vaatisi vastauksia seuraaviin kysymyksiin:

- Onko tietoturvallisuuden tila parempi tänä vuonna kuin viime vuonna?
- Mitä vastinetta tietoturvallisuuteen sijoitetuille rahoilleen organisaatio saa?
- Miten eri liiketoimintayksiköiden tietoturvallisuutta voidaan vertailla?

Perinteisiä keinoja etsiä vastausta Jaquithin (2007, s. 12) esittämiin kysymyksiin ovat monitorointi ja auditointi. Mittaamisen ohella monitorointi antaa johtamisen näkökulmasta tarvittavaa tietoa tietoturvallisuuden tilasta. Monitorointi tarkoittaa yksinkertaistetusti sitä, että kiinnitetään huomioita tietoturvallisuuteen, eli valvotaan että tietoturvatoiminnot toimivat tarkoituksenmukaisesti. Esimerkiksi videovalvonta on monitorointia, mutta myös mittareita voidaan monitoroida. Reaaliaikainen monitorointi on tehokas tapa saada tarvittavaa tietoa tietoturvallisuuden tilasta, mutta se on kaikista kallein keino. Toisaalta reaaliaikainen monitorointi on hyödytöntä, mikäli ei osata määritellä viitekehystä sille, milloin valvottavan kohteen tietoturvallisuuden tila on hyvä ja milloin huono. Usein jokin kohde vaatii monitorointia siksi, että niille ei ole saatavilla mittareita. Toiset kohteet taas vaativat mittaamisen tukena monitorointia, mikäli ne ovat todella kriittisiä tai mittarit ovat vasta kehitysasteella ja siksi epäluotettavia tai epätarkkoja. (Brotby 2009.) Käytännön esimerkki kohteesta, jota on haastava mitata, on kulunvalvonta palvelinsaleihin. Sen lisäksi, että palvelinsaleihin pääsyksi vaaditaan tunnistautuminen, käytetään myös valvontakameroita. Näin jälkikäteen on mahdollista osoittaa väärinkäytöksiä. Monitorointi eroaa siis mittaamisesta siten, että se on tapahtumien valvontaa. Brotbyn (2009, s. 18) mukaan mittarit ovatkin yksi tapa monitoroida tietoturvamenetelmiä, lisäksi mittaaminen on usein kustannustehokkaampaa kuin monitorointi ja säästää organisaation resursseja.

Auditointi perustuu usein ISO/IEC 27001 tai vastaavaan standardiin, jonka avulla organisaatiot voivat tunnistaa tietoturvallisuuteen liittyviä vaatimuksia. Standardi on siis tehty auditoijien näkökulmasta ja sen perusteella arvioidaan, toteutuuko organisaation tietoturva standardin asettamien tavoitteiden mukaisesti. (Jaquith 2007, s. 30.) Esimerkiksi tietoturvatavoite ”Turvallisuudesta huolehtiminen asiakassuhteista” ohjeistetaan

standardissa seuraavasti: ”Kaikista tunnistetuista turvallisuusvaatimuksista tulee huolehtia, ennen kuin asiakkaalle annetaan pääsy organisaation tietoon tai suojattaviin kohteisiin” (ISO/IEC 27001). Mittarina tätä tavoitetta, kuten ei muitakaan, voida käyttää, vaan niiden tulkitseminen riippuu täysin auditoijasta. Vaikka Jaquith (2007, s. 28-30) kritisoikin ISO/IEC 27001 käyttämistä mittarina tai sen perustana, saattaa se olla hyvä lähtökohta tunnistaa organisaatiolle tärkeitä tietoturvatoimintoja. Brotby (2009, s. 89) mainitsee, että ISO/IEC 27001 voi tarjota perustan muodostaa käsitys siitä, mikä on tietoturvallisuuden tavoite tila. Kuten mittarin kehitysprosessia esitellessä mainittiin, tulee mittareita suunnitellessa tunnistaa strategiaan liittyviä tavoitteita ja asettaa niiden mukaan tavoitteet mitattavalle asialle. Organisaation on itse määriteltävä, miten se standardeja tai niiden kautta saatavia auditointituloksia käyttää. Auditointitulokset voisivatkin tarjota tietoturvamittareille aihealueita, joiden kautta tietoturvallisuuden tilaa esitettäisiin johdolle.

Tietoturvamittareiden avulla pyritään siis arvioimaan organisaation tietoturvallisuuden tilaa. Niitä voidaan hyödyntää useaan eri tarkoituksiin tukemaan arviota siitä, kuinka hyvä tietoturvallisuus on eri näkökulmista. Kattavin näkökulma on koko organisaation, sen tuotteiden ja prosessien tietoturvallisuuden tila, jota tietoturvamittareilla pystytään tarkastelemaan. Tietoturvamittarien avulla tuetaan riskienhallinnan työtä, kun pystytään arvioimaan onko tietoriskejä onnistuttu pienentämään. Tietoriskejä hallitaan tietoturvamenetelmien avulla, joiden ominaisuuksia vertaillaan mittareiden avulla. Mittareita voidaan käyttää testauksen ohessa, esimerkiksi järjestelmien testauksen tai suojausmenetelmien testauksen tukena. Ulospäin näkyvin mittari tietoturvallisuuden tilasta on mittari, jota käytetään sertifikaattien saamisen tukena ja organisaation toiminnan evaluoinnin osana. (Savola 2007)

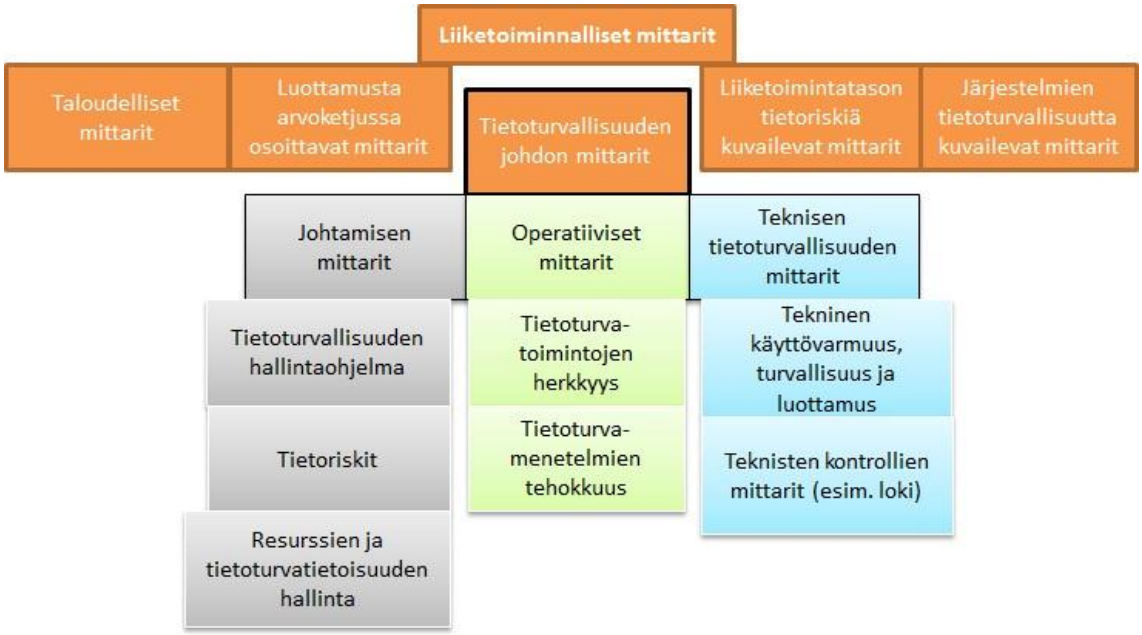
4.2 Tietoturvallisuuden mittaamisen osa-alueet

Tietoturvallisuuden mittaaminen voidaan jakaa osa-alueisiin. Esimerkiksi tietoliikenteestä, ohjelmistoista ja laitteistoista saadaan helposti vaikkapa saatavuuteen liittyvää dataa. Tällainenkin data voi olla hyödyllistä liiketoiminnalle, mikäli kyseessä on liiketoiminnalle kriittinen järjestelmä. Tällaisia mittareita käsitellään kuitenkin yleisesti teknisinä tietoturvamittareina operatiivisten työntekijöiden työn tueksi. Koko organisaation tukena käytetään mittareita, joiden avulla kuvaillaan ja jäljitetään organisaation tietoturvatoimintojen, ohjelmien ja prosessien tehokkuutta tietoturvallisuuden näkökulmasta. Näitä voidaan pitää enemmänkin johtamisen mittareina. Teknisten ja johtamisen mittareiden lisäksi perinteiseen jaotteluun kuuluu vielä operationaaliset mittarit, joiden käyttö on hieman lähteestä riippuen riskienhallinnallinen näkökulma. (mm. Henning 2001; Vaughn et al. 2003; Swanson et al. 2003)

Savola (2007) on muodostanut muun muassa edellä esitellyn jaottelun perusteella korkean tason jaottelun, jonka avulla pyritään liittämään alimman tason teknisiä yksityis-

kohtia kuvastavat mittarit osaksi kokonaisuutta. Korkeimmalla tasolla Savolan (2007) jaottelussa ovat liiketoiminnalliset mittarit. Näiden mittareiden kehittämistä ohjaavat liiketoiminnan tavoitteet, joita pyritään mittareiden avulla viemään alemmille tasoille. Esimerkkejä näistä liiketoiminnallisista tavoitteista, jotka vaikuttavat tietoturvallisuuteen, esiteltiin tietoturvastrategiaa ja politiikkaa käsittelevässä luvussa 2.4. Liiketoiminnalliset mittarit voidaan edelleen jakaa viiteen eri alaluokkaan. Taloudelliset mittarit, kuten investoinnille saatava tuotto (ROI) ja muut investointeja käsittelevät mittarit, ovat liiketoiminnalle tärkeitä mittareita. Näitä ei kuitenkaan käsitellä enää alemmilla tasoilla. Luottamusta kuvastavat mittarit ovat tärkeitä mittareita liiketoiminnalle, jotka kuvailevat minkälainen kuva tietoturvallisuudesta yrityksen arvoketjusta muodostuu. Riskien hallintaan liittyvät mittarit taas nostavat pinnalle niitä asioita tietoturvallisuuden viitekehyksestä, jotka saattavat nousta liiketoiminnallisiksi riskeiksi. Lopulta tietoturvallisuuden tilaa kuvailevat mittarit, jotka koostetaan tietoturvapäällikön mittareista ja mittarit, jotka kuvailevat korkean tason vaatimuksia palveluille järjestelmille ja prosesseille. Näitä mittareita ovat esimerkiksi käyttövarmuus, turvallisuus ja luottamus. (Savola 2007.)

Toinen taso Savolan (2007) jaottelussa liiketoiminnallisten tietoturvamittarien jälkeen on tietoturvallisuuden johdon mittarit. Käytännössä nämä voisivat olla mittareita, joita tietoturvapäällikkö ja muut henkilöt, joilla on vastuu tietoturvallisuudesta, käyttävät. Esimerkiksi prosessien tai järjestelmien omistajat voisivat olla henkilöitä, jotka käyttävät toisen tason mittareita, kun taas palvelun omistajat tarvitsevat työssään kokoelmaa sekä ensimmäisen ja toisen tason mittareista. Kuvassa 4.1 esitellään tietoturvamittarien jaottelu.



Kuva 4.1. *Tietoturvamittareiden luokittelu. (Mukailtu lähteestä Savola 2007)*

Savolan (2007) muodostama jaottelu ulottuu kuvan 4.1 mukaisesti vielä kolmannelle tasolle. Kolmannen tason mittarit voisivat olla jossain prosessien haltijoiden mittareita, varsinkin operatiiviset mittarit ja tietojärjestelmien tilaa kuvailevat mittarit. Näiden avulla voidaan ymmärtää mitä käytännön tasolla tapahtuu. Johtamisen mittareiden avulla voidaan ymmärtää, mikä on koko organisaation tietoturvallisuuden tila ja seurata, kehittyykö se suunnitellusti.

Mittareiden liittäminen liiketoimintaan nähdään tieteellisessä tutkimuksessa tärkeänä ja mittareiden jaottelua pyritään muodostamaan liiketoimintalähtöisesti. Center for Internet Security (CIS) on usean tuhannen tietoturva-ammattilaisen muodostama yhteisö, joka tarjoaa vertailukohtia yritysten tietoturvallisuuteen ja pyrkii kehittämään tietoturvamittareita (CIS 2012). Yhteisön mukaan tietoturvallisuuden ongelmana on tehdä kustannustehokkaita päätöksiä, koska tietoturvallisuudesta puuttuu laajasti hyväksytyt, yksiselitteiset mittarit. Tähän tarpeeseen on muodostettu jaottelu erilaisista liiketoimintaan liittyvistä tehtävistä. Toisin kun tieteellisissä lähteissä, näihin on liitetty esimerkkimittareita. CIS:n muodostama esimerkkimittaristo esitellään taulukossa 4.1.

Taulukko 4.1. *CIS -yhteisön muodostamat tietoturvamittarit*

Liiketoimintaan liittyvä tehtävä	Esimerkkimittari
Tietoturvatapahtumien hallinta Kuinka hyvin ja tarkasti, havaitaan, ratkaistaan ja toivutaan tietototurvataphtumista.	• Keskiaika tietoturvatapahtumien havaitsemiseen • Tietoturvatapahtumien määrä • Keskiaika tietoturvatapahtumien välillä • Keskiaika tietoturvatapahtumien korjaamiselle
Heikkouksien hallinta Miten hyvin hallitaan heikkouksien tunnistaminen ja niihin reagointi	• Heikkouksien tunnistamisen laajuus • Niiden järjestelmien osuus, joissa ei ole tunnistettuja vakavia uhkia • Keskiaika havaituilta uhilta suojautumiseen • Tunnettujen heikkouksien määrä
Päivitysten hallinta Kuinka hyvin ylläpidetään järjestelmien päivityksiä	• Päivityspolitiikan vaatimustenmukaisuus • Päivitysten hallinnan kattavuus • Keskiaika järjestelmien päivittämiselle
Sovellusten turvallisuus Voidaanko liiketoimintasovellusten suunnitelman mukaista käyttöä varmistaviin tietoturvatoimintoihin luottaa	• Sovellusten määrä • Kriittisten sovellusten osuus sovelluksista • Riskiarvioitujen sovellusten osuus • Turvallisuustestauksen kattavuus
Muutostenhallinta Miten muutokset järjestelmiin vaikuttavat tietoturvallisuuden tilaan	• Muutosten toteutukseen kuluva aika • Niiden muutosten osuus, jossa tietoturvallisuus on huomioitu • Niiden muutosten osuus, jotka aiheuttavat tietoturvatapahtuman
Liiketoiminnalliset mittarit Mikä on tietoturvallisuuden kustannustaso ja mihin investointeja tehdään	• Tietoturvallisuus budjetin osuus IT-budjetista • Tietoturvabudjetin allokointi

CIS (2009) esittelemä esimerkkimittaristo on selkeästi suunnattu tietoturvapäällikölle. Näiden pohjalta olisi varmasti mahdollisuus nostaa esille tärkeimpiä asioita ja koostaa kuvaa tietoturvallisuuden tilasta liiketoimintajohdolle. Esimerkiksi ongelmien suhteen voisi koostaa yhden mittarin. Tämän mittarin voisi taas liittää osaksi heikkouksien tunnistamista ja sitä, miten sovellusten hallinta etenee näiden asioiden ohella. Päivittäminen taas on liian tekninen asia esitettäväksi liiketoimintajohdolle. CIS (2009) esittelemät

mittarit taas ovat hyvin vaikea toteuttaa, mikäli organisaatio ei ole tunnistanut järjestelmiään riittävän tarkalla tasolla, jolloin päivitysten laajuutta tai keskiaikaa ei voida mitata. Toisaalta Lemos (2012) mainitsee, että mittari joka kertoo järjestelmien päivitykseen kuluvan ajan, indikoi hyvin kuinka hyvin organisaatio tuntee tietotekniikka-arkkitehtuurinsa. Mikäli päivityksen mittarit liitetään liiketoimintaan, esimerkiksi liiketoimintakriittisten palveluiden saatavuuteen, voisi mittari olla myös liiketoimintajohdolle relevantti. Jaquith (2007, s. 55) ja Lemos (2012) esittelevät päivittämiseen liittyvän mittarin, joka seuraa kuinka usein kriittisissä järjestelmissä tehdään suunnittelemattomia päivityksiä. Tämä mittari on suoraan sidoksissa liiketoimintaan ja sen sujuvuuteen.

Lemos (2012) esittelee päivittämiseen liittyvien mittareiden lisäksi kolme muuta tietoturvamittaria, jotka hänen mukaan luokitellaan strategisiksi. Näistä tietoturvabudjetin osuus IT-budjetista vastaa CIS (2012) mittaristoon kuuluvaa mittaria. Standardoitujen järjestelmien osuus kaikista järjestelmistä taas on mittari, joka liitetään edellä esiteltyyn yhdistelmään sovellusten ja järjestelmien riskikartoituksista sekä heikkouksien hallinnasta. Kolmas mittari taas pyrkii kuvailemaan, kuinka nopeasti työntekijät kuittaavat kriittisimmät asiakasvaatimukset tai palvelutasoon liittyvät vaatimukset eri prosessien ohella, joihin nämä liittyvät. Tieto tähän mittariin kerätään tarkistuslistojen avulla.

Kowalski & Barabanov (2011) kritisoivat olemassa olevia luokitteluja siitä, että luokittelujen väliset suhteet jäävät usein hämärän peittoon. Poikkeuksena tästä mainitaan kuvassa 4.1 esitetty Savolan (2007) muodostama jaottelu, jossa korkean tason luokittelu on edelleen jaettu alemman tason kategorioihin. Toinen mainittu ongelma luokitteluissa on, että tekniset ja pehmeät mittarit eritellään täysin. Tämä johtaa siihen, että molempia osa-alueita kuvailevia mittareita ei pystytä tulkitsemaan riittävän laajasti. Esimerkiksi sisäisten järjestelmien ongelmien määrää kuvaileva mittari voi osoittaa tehokkaiden tietoturvamenetelmien lisäksi sitä, että organisaation järjestelmiin liittyvää käyttöpolitiikkaa on tiukennettu. Mittari voi myös osoittaa, että työntekijöiden ymmärrys ongelmiin johtavista asioista on parantunut ja tästä syystä ongelmien määrä on vähentynyt. Kowalskin & Baranovin (2011) mukaan käytännönläheisimmän jaottelun, jossa tietoturvamittarit esitellään maturiteettitason mukaisesti, ovat muodostaneet Chew et al. (2007). Tässä jaottelussa mittarit ovat joko kehittämiseen liittyviä, suorituskykyyn liittyviä tai liiketoiminnallisia vaikutuksia mittaavia. Chewn et al. (2007) luokittelun mukainen mittaaminen esitellään tässä tutkimuksessa osana tietoturvallisuuden mittaamisen prosessia, sillä sen nähdään kuvailevan kuinka hyvin mittareita on onnistuttu ottamaan käyttöön.

4.3 Miksi tietoturvallisuutta mitataan?

Tietoturvallisuuden mittaamisen voi perustella samasta syystä kuin mittaamisen yleisesti. Mittaaminen antaa tietoa organisaation toiminnasta päätöksen teon tueksi. Brotby (2009) näkee mittaamisen olevan aina johtamisen tukitoimi. Jaquith (2007, s. 11) esitte-

lee tietoturvallisuuden mittaamisen liiketoimintapaineiden kautta. Ensinnäkin tiedon muuttuminen yhä kriittisemmäksi tuotannontekijäksi lisää tarvetta ymmärtää paremmin tietoturvallisuutta ja osoittaa sen toimivuus. Toimivuutta ei pystytä osoittamaan ilman mittareita, eikä tästä syystä voida nähdä miten hyvin eri tietoturvatoiminnot tai työkalut toimivat organisaatiossa. Tästä syystä mittareita tarvittaisiin osoittamaan, kuinka paljon ja mihin organisaation kannattaa tietoturvallisuuden näkökulmasta investoida. Mittareiden avulla pyritään siis poistamaan tietoturvallisuuteen liittyvää epävarmuutta ja epätietoisuutta. Mittareiden avulla voidaan arvioida tietoriskejä, ymmärtää tietoturvallisuuden suorituskyky ja arvioida tietoturvallisuuden kustannuksia.

Toisaalta tietoturvallisuutta kannattaa mitata, jotta osoitetaan läpinäkyvyyttä ja vastuullisuutta tietoturvallisuudesta. Näitä seikkoja vaaditaan alan normistossa, laeissa, asiakkaan tai muiden sidosryhmien toimesta. Toisin sanoen vaatimustenmukaisuuden osoittaminen on tärkeä peruste mittaamiselle, jolloin varmistetaan toiminnan lainmukaisuus, sidosryhmien tyytyväisyys ja yrityksen omien tavoitteiden täyttyminen. (Jaquith 2007, s. 11; Barabanov et al. 2011; Kowalski & Barabanov 2011; Savola et al. 2012; ISO27004.) Lisäksi läpinäkyvyys ja vastuullisuuden osoittaminen lisää sidosryhmien luottamusta organisaation toimintaan. Johdon päätöksen tekoon tämä vaikuttaa siten, että vaatimustenmukaisuutta kuvastavien mittareiden perusteella pystytään kohdistamaan resursseja paremmin. Mittaamisen avulla on mahdollista perustella ja priorisoida tietoturvainvestointeja sen perusteella, mistä on eniten hyötyä ja mikä on kustannustehokkain tapa liiketoiminnan suojaamiseen. (Brotby 2009, s. 5; Kowalski & Barabanov 2011.) Mittareiden kautta voidaan arvioida, kuinka hyvin siihen käytetyt panostukset vaikuttavat ja ymmärtää syy-seuraus suhteita toteutettujen toimenpiteiden ja tietoturvallisuuden tilan välillä. Tämän avulla tietoturvallisuutta ja siihen liittyvää osaamista voidaan kehittää sen vaikuttavuuden ja tehokkuuden näkökulmasta. (Brotby 2009, s. 5: Barabanov et al. 2011; Savola et al. 2012.)

Tietoturvatoimintojen tulee olla linjassa organisaation strategian ja muun toiminnan kanssa, johon mittaamisella halutaan vaikuttaa (Brotby 2009, s. 5). Kuten luvussa 2.6 perusteltiin, tietoturvallisuuden tilan ymmärtäminen suhteessa strategiaan ja kustannuksiin on tärkeää, jotta voidaan asettaa sille tavoitteita. Kowalski & Barabanov (2011) perustelevat mittaamisen tärkeyttä sillä, että tulosten avulla on mahdollista asettaa tavoitteita tietoturvallisuudelle, ellei niitä ole aikaisemmin osattu määritellä. Mittareiden avulla pyritään yhteen sovittamaan tietoturvallisuutta osaksi muita organisaation tavoitteita ja varmistaa näin, että tietoturvallisuus ei aiheuta ylimääräisiä kustannuksia ja toisaalta pystyä ymmärtämään tietoturvallisuutta kokonaisuutena. Yhtenäinen mittaristo kaventaisi liiketoiminnan ja tietoturvallisuuden välistä kuilua sekä tarjoaisi kvantitatiivisen ja objektiivisen perustan tietoturvallisuudelle. (Savola 2007; Kowalski & Barabanov 2011; Savola et al. 2012). Savola (2010) huomioi, että tietoturvallisuuden mittaaminen mahdollistaa ennakoivan tietoturvallisuuden hallinnoinnin ja tarjoaa keinon kommunikoida tietoturvallisuudesta organisaation sisällä. Kommunikointi ja ennakoitavuus tar-

joavat mahdollisuuden lisätä ymmärrystä tietoturvallisuudesta läpi organisaation, jonka avulla tietoturvallisuuden tilaa voidaan edelleen parantaa.

Ongelmien löytäminen tärkeä peruste mittaamiselle, sillä mittaaminen tarjoaa mahdollisuuden analysoida ja tunnistaa ongelmiin johtavia syitä. Analysoinnin avulla voidaan kehittää tietoturvallisuutta ja suunnitella uusia tietoturvatoimintoja, joilla vastataan uusiin haasteisiin ja vaatimuksiin. (Datta & Banerjee 2011.) Tietoturvallisuuden mittaamisella tuetaan organisaation tietoturvallisuuden hallintaa monin eri tavoin, löytää kehityskohteita, arvioida ja kehittää tietoturvallisuuden tilaa, viestiä henkilöstölle tavoitteita ja seurata tietoturvatoimintojen suorituskykyä. Nämä syyt mitata tietoturvallisuutta ovat samoja kuin mittaamisen käyttötarkoitukset yleisesti. Luvussa 3.2 pohdittiin mittaamista osana johtamisjärjestelmää, jossa perusteltiin mittareiden käyttö strategian jalkauttamiseen, henkilökunnan motivointiin ja tavoitteiden asettamiseen. Tietoturvamittarit sopivat kirjallisuuden mukaan hyvin samankaltaisiin tarkoituksiin, mutta tietoturvamittareiden asettamisessa on huomattavia haasteita. Selkein erikoispiirre tietoturvallisuuden mittaamisessa on tietoturvallisuuteen kohdistuvat vaatimukset ja niiden täyttämisen osoittaminen eri sidosryhmille.

4.4 Haasteet tietoturvallisuuden mittaamisessa

Tietoturvallisuuden mittaaminen on vähän tutkittu aihealue eikä sitä ole vielä täysin pystytty viemään käytännön tasolle. Mittareiden määritteleminen on huomattavan vaikeaa, koska tietotietoturvallisuuden aihepiiri on laaja, jolloin mittaustavoitteita on hankala asettaa. Savola (2007) kuvailee ongelman olevan siinä, että tietoturvallisuuden johtamista ja liiketoimintajohtamista käsitellään erillisinä aiheina samaan aikaan, kun myös tietoturvallisuuden osa-alueiden käsittely on usein erillistä ja painottuu tietotekniikkaan. Lisäksi tietoturvapäällikön työ on usein reaktiivista, jolloin työaikaa ei jää kokonaisuudenhallinnalle (Kairab 2005). Näistä syistä kokonaisvaltaista kuvaa tietoturvallisuuden tilasta on vaikea määritellä ja mittarit koetaan usein ylimääräiseksi taakaksi (Savola et al. 2012). Mittareita ei ole Savolan et al. (2012) mukaan myöskään voitu edelleen kehittää käytännön kokemusten perusteella, sillä niitä ei ole päästy kokeilemaan tai implementoimaan riittävästi käytännössä.

Koska tietoturvallisuus koetaan erillisenä aihealueena, ja tietoturvallisuus on usein tukifunktio osana tietohallintoa, oikean kohdeyleisön löytäminen mittareille voi osoittautua haasteeksi. Pironti (2007) esittää, että jos mittareiden tuloksien avulla tietoturvallisuudesta viestitään väärälle kohdeyleisölle, on se ensinnäkin resurssien tuhlausta ja toisaalta saattaa aiheuttaa sekaannusta ja vaikeuttaa päätöksentekoa. Myös Jaquithin (2007, s. 25) ja Ryanin & Ryanin (2008) mukaan turhan ja epärelevantin datan kerääminen kasvattaa huonoista päätöksistä johtuvaa riskiä. Esimerkiksi teknisten tietoturvamittarien esittäminen johdolle ei ole relevanttia. Yrityksessä saatetaan joutua tilanteeseen, jossa liiketoiminnan näkökulmasta mittarit palvelevat vain tietoturvapäällikön työtä, jolloin

investointeja niihin ei tehdä. Herrmann (2007) ja Brotby (2009, s. 10) painottavatkin, että mittareita suunniteltaessa pitää olla hyvä ymmärrys siitä, ketkä ovat niiden kohdeyleisö ja keskustelut kehityssuunnitelmineen on käytävä sekä heidän kanssa että heidän näkökulmasta.

Yksi tietoturvallisuuden mittaamisen haasteista on se, että mittarit muodostava väärän kuvauksen organisaation tietoturvallisuuden tilasta. Tästä johtuen johto saa epärealistisen kuvan tietoturvallisuudesta ja riski tehdä huonoja päätöksiä kasvaa. Nämä aiheutuvat sekä edellä esitetyistä seikoista, kuten siitä että epärelevantin datan keräämisestä. Usein tietoturvallisuutta mitataan helposti mitattavia asioita sen sijaan, että mitattaisiin liiketoiminnalle tärkeitä asioita, joka ei ensinnäkään tuo lisäarvo johdon päätöksenteolle tai toisaalta kuvaile organisaation tietoturvallisuuden tilaa. Mittaamista tulisikin suunnitella liiketoimintalähtöisesti. (Kowalski & Barabanov 2011.) Savolan et al. (2012) mukaan tietoturvallisuuden tehokkuuden mittaaminen perustuu aina arvioon sen oikeellisuudesta, eli tietoturvallisuuden tehokkuutta ei voida mitata absoluuttisesti. Tämä johtuu sekä tiedon puutteesta, huonosti tietoturvallisuuden kattavasta mittaamisesta ja mittaajien ennakkoasenteista mittauksen kohteeseen liittyen. Toisaalta tietoturvallisuuden voidaan olettaa olevan kunnossa niin kauan kun siihen liittyvät ongelmat eivät vaikuta liiketoimintaan. Jansenin (2009) mukaan tulosten manipulointi omien tavoitteiden mukaiseksi on suuri riski tietoturvallisuutta mitattaessa. Näin ollen tulosten luotettavuus ja validiteetti voivat olla heikkoja. Tietoturvallisuutta mitattaessa on todella tärkeää kiinnittää huomiota mittareiden oikeellisuuteen.

Kuten edellä mainittiin ja luvussa 2.3.1 esiteltiin, johdon näkökulmasta tietoturvallisuus on usein tukifunktio jota ei osata liittää osaksi muuta liiketoimintaa. Tällöin tietoturvallisuuden mittaamiselta puuttuu johdon tuki, joka on kriittinen menestystekijä tietoturvallisuudelle, sen toteuttamiselle ja yleisemmin koko organisaation asenteelle tietoturvallisuutta kohtaan (Kairab 2005, s. 50). Nämä tekijät heijastuvat mittaamiseen ja motivaatioon mitata tietoturvallisuutta. Huono motivaatio mitata tietoturvallisuutta on jo itsessään yksi haaste. Brotby (2009, s. 63) mainitsee, että tietoturvaongelmia ei perinteisesti raportoida kovin laajalti, sillä tällä saattaa olla vaikutuksia maineeseen ja osakearvoon. Tästä syystä kattavaa historiallista dataa ei välttämättä ole saatavilla mittaamisen tai tavoitteiden asettamisen tueksi. Toisaalta mittareiden antamia huonoja tuloksia saatetaan pelätä, jolloin niitä ei myöskään haluta saada (Herrmann 2007). Vaikka dataa tietoturvallisuuden mittaamiselle olisi olemassa ja sitä kerättäisiin, haasteita muodostavat jatkuvasti muuttuvat tietoturvavaatimukset ja tavoitteet, joiden perusteella tietoturvatoimintoja kehitetään, ja toimintaympäristö, jota tietoturvatoimintojen tulisi suojata (Pironti 2007; Barabanov et al. 2011).

Kriittisin haaste tietoturvallisuuden mittaamisessa on, niiden mittausten ulkopuolelle jätettyjen asioiden vaikutusta tietoturvallisuuteen ei voida täysin ymmärtää. Toisin sanoen mittaamista saatetaan suorittaa täysin väärin painoaluein, liian suppeasti tai ei osa-

ta arvioida, mitkä asiat mittariin lopulta vaikuttavat. (Brotby 2009, s. 65.) Esimerkiksi virustorjunnassa osataan mitata löydettyjen virusten määrää, muttei välttämättä osata sanoa kuinka monta virusta ohitti suojauksen. Tämä mittari on huono kertomaan mitään tietoturvallisuuden tilasta, sillä sitä ei voida liittää liiketoimintaan eikä tieto virusten määrästä tuo lisäarvoa tietoturvapäällikölle. Edellä kuvatun kaltainen ongelma konkretisoituu varsinkin silloin kun yritys ei ole tunnistanut prosessiensa tiedon suojaamisen tarvetta liiketoimintalähtöisesti. Brotby (2009, s. 84) tiivistää ongelman syyksi, että mittareita ei voida muodostaa, jollei tietoturvallisuuden hallinnointia ole organisoitu. Luvussa 2.5 esiteltiin asioita, jotka liittyvät tietoturvallisuuden hallinnointiin. Tietoturvamittareita on käsitelty hyvin vähän liiketoiminnan näkökulmasta, mikä aiheuttaa osaltaan haasteita tietoturvallisuuden tilan korkean tason kuvaamiselle. Esimerkiksi ISO/IEC 27004 standardissa, jossa käsitellään tietoturvallisuuden mittaamista, esitellään yksi mittari jonka kohdeyleisönä on johtoryhmä. Tämä mittari kuvailee fyysisen pääsynhallinnan tasoa.

Tämän tutkimuksen kannalta mielenkiintoisen ongelman esittelee Jaquith (2007, s. 28-30). Hänen mukaan vaatimustenmukaisuutta ei voida mitata tai erilaisia tietoturvallisuuteen liittyviä standardeja ei voida käyttää mittaamisen tukena. Perusteluja tälle on muun muassa se, että niiden toteutumista seurataan subjektiivisesti ja ne auttavat lähinnä tunnistamaan tietoturvallisuuteen liittyviä toimenpiteitä. Toisaalta standardit jättävät paljon tulkinnan varaa organisaatiolle eivätkä ohjeista mittaamisessa. Jansen (2009) huomauttaa, että subjektiivinen mittaaminen perustuu usein mittaajan kokemukseen ja taitoihin, eikä se sen takia ole välttämättä toistettavissa. Tämä antaa haasteen mittareiden luotettavuuden arvioinnille. Sekä Jaquith (2007, s. 30) että Brotby (2009, s. 65) kritisoivat myös sitä, että standardin mukaisuus ei lähtökohtaisesti paranna tietoturvallisuutta, vaan tietoturvallisuuden parantuminen on lähinnä sivuvaikutus. Brotby (2009, s. 65) perustelee tämän sillä, että standardin mukaisuus ei välttämättä kerro, sopiiko tietoturvallisuudenhallintamalli siihen tukeutuvalle organisaatiolle. Chapin & Akridge (2005) lisäävät, että vaikka organisaatio olisi saavuttanut tietyn standardin mukaisen vaatimustason, ei se tarkoita että sitä toteutettaisiin onnistuneesti päivittäisen toiminnan osana. Brotby (2009) esittää, että standardin mukaisuutta voidaan verrata lentoliikenteeseen: lentokoneiden standardien mukainen lentokelpoisuus ei kerro lentääkö kone oikeaan suuntaan.

Jaquithin (2007) ja Brotbyn (2009) mielipiteet ovat mielenkiintoisia. Ensinnäkin Jaquith argumentoi, että ongelma on, että organisaatiot joutuvat itse tunnistamaan ja räätälöimään tietoturvatoiminnot. Brotby taas näkee ongelmana, että standardin seuraaminen ei välttämättä sovi organisaation toimintaan. Näkökulmissa on selvä ristiriita. Voisi päätellä, että standardin seuraaminen siten, että johdon ja tietoturvapäällikön näkökulmasta on tunnistettu tietoturvatavoitteet, nimenomaan sopii organisaation toimintaan. Toisaalta tietoturvallisuuden parantuminen on varmasti toivottu sivuvaikutus standardin mukaisuudelle, eikä niiden tehtävänä ole ohjeistaa sitä, miten organisaation toimintaa pitäisi mitata. Kolmanneksi vertaus lentoliikenteeseen ei ole relevantti, koska se on suunnattu

huonosti. Johdon näkökulmasta ei ole tärkeää seurata aktiivisesti lentääkö koneet oikeaan suuntaan, vaan lentävätkö lentoyhtiön koneet tavoitteen mukaisesti lentokentältä toiselle. Parmenter (2006) esittelee lentoliikenteeseen liittyvän kriittisen menestystekijän ”oikea aikaiset lähdöt ja nousut”, jota mitataan myöhästyneiden koneiden määrällä. Tämän menestystekijän kautta eräs lentoyhtiö onnistui vähentämään merkittävästi ongelmia, jotka liittyivät lentokoneiden myöhästelyyn. Tietoturvallisuuden näkökulmasta johdon tulee siis tietoturvallisuuteen liittyvien yksityiskohtien sijaan määrittää, minne tietoturvallisuuden suhteen ollaan menossa ja päästäänkö sinne tavoitellusti. Toisaalta johdon tulee myös varmistaa, että yhtiö ”lentää turvallisilla koneilla”, eli että yhtiön tietoturvallisuus on riittävän hyvällä tasolla. Tietoturvapäällikkö on tässä tapauksessa pilotti, joka tarvitsee yksityiskohtaisempaa tietoa organisaation toiminnasta. Haasteena on loppujen lopuksi pitää se, että ilman annettuja tavoitteita ja päämääriä tietoturvallisuudelle, tietoturvapäällikkö ei voi ohjata organisaation tietoturvallisuutta.

4.5 Tietoturvallisuuden mittaaminen organisaatiossa

Tietoturvallisuuden mittaamisen aloittaminen ilman tietoturvallisuuden dokumentointia, riittävän tarkasti kuvattuja prosesseja ja toimintatapoja on haastavaa, mikäli halutaan kerätä kvantitatiivista dataa. Kun toimintatavat vakiintuvat ja niitä ymmärretään paremmin, voidaan prosessien suoriutumista mitata eri tavalla, kuin vakiintumattomien toimintatapoja. Ensimmäinen askel tietoturvallisuuden mittaamiseksi onkin tavoitteiden asettaminen, prosessien tunnistaminen ja tietoturvatoimenpiteiden vakiinnuttaminen. (Chew et al. 2007.) Toimenpiteiden vakiinnuttamista ja tietoturvallisuuteen vaikuttavia asioita pohdittiin luvuissa 2.4 ja 2.5. Tätä vakiinnuttamista voidaan tukea implementaation etenemistä kuvaavilla mittareilla, jotka muodostavat perustan muiden mittareiden kehittämiselle. Mittaamisen voidaankin nähdä kehittyvän maturiteettitason kasvaessa. Kun prosessit ja toimintatavat ovat riittävällä tasolla, pystytään niiden suorituskykyä mittaamaan. Tämän jälkeen on mahdollista siirtyä ennakoivampien mittareiden käyttöön, jotka arvioivat tietoturvatapahtumien vaikutuksia ja riskejä. (Chew et al. 2007; Lippmann et al. 2012.) Lippman et al. (2012) pohtivat maturiteettitasoja tietojärjestelmien kautta, kun taas Chew et al. (2007) pohtivat tietoturvallisuuden hallinnan kautta. Kuvassa 4.2 on esitetty tietoturvallisuuden mittaamisen prosessi maturiteetin näkökulmasta.

Kuva 4.2. *Tietoturvamittareiden maturiteettitasot. (Mukailtu lähteistä Chew et al. 2007; Lippmann et al. 2012)*

Mittareiden kehittämisen ensivaiheessa keskitytään seuraamaan, miten tietoturvallisuuteen liittyvät kehitysprojektit etenevät. Tässä vaiheessa järjestelmän omistajat arvioivat, mitkä ovat suurimmat uhat, jotka liittyvät järjestelmiin. Tämän jälkeen pyrkiä määritelmään prosesseja, implementoimaan uusia tietoturvatoimintoja ja pohtia, mistä pystytään kerätä mittausdataa. (Chew et al. 2007; Lippmann et al. 2012.) Mittareita ensimmäiselle tasolle ovat esimerkiksi niiden järjestelmien prosenttiosuus, joiden tietoturvasuunnitelma on hyväksytty ja niiden palvelimien prosenttiosuus eri järjestelmissä, joissa on vaaditun mukaiset asetukset. Dataa implementoinnin edistymiseen voidaan saada tietoturvallisuuteen liittyvistä arviointiraporteista, projektien edistymistä kuvaavista raporteista ja muista dokumenteista, jotka tiedottavat tietoturvallisuuden kehittymisohjelmista. (Chew et al. 2007.) Lippman et al. (2012) lisäävät tarkistuslistojen käytön osana kehitysprojekteja, joiden avulla on helppo seurata miten tavoitteiden toteuttaminen etenee.

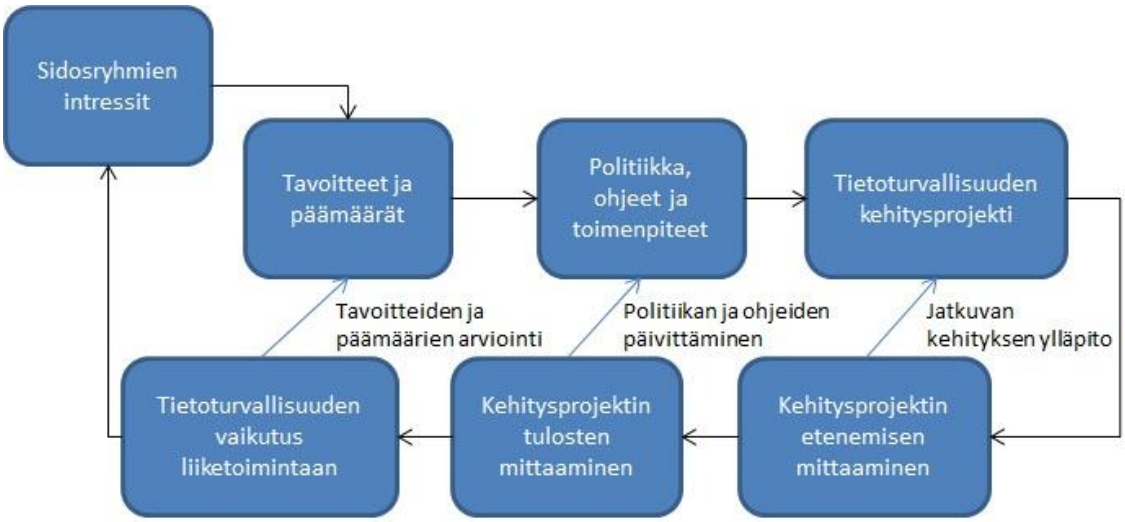
Toisessa vaiheessa pyritään mittaamaan tietoturvallisuuden suorituskykyä. Näkökulmana tähän on se, miten hyvin vakiintuneet toimintatavat ja prosessit suoriutuvat. Tässä vaiheessa voidaan tutkia toimivatko prosessit oikean aikaisesti, kattavatko ne tarpeeksi hyvin tietoturvallisuuden eri osa-alueita ja toisaalta, ovatko mittarit riittävän tarkkoja. (Chew et al. 2007; Lippmann et al. 2012.) Lippmannin et al. (2012) mukaan mittauksilla arvioidaan todellisen tietoturvan tilan suhdetta tavoiteltuun tilaan. Chew et al. (2007) taas kuvailevat, että mittareiden avulla arvioidaan, kuinka hyviä päätöksiä tietoturvallisuuden suhteen on aikaisemmin tehty ja pohtia, miten tietoturvallisuuden tasoa on mahdollista parantaa. Toisin sanoen tämän maturiteettitason mittareilla voidaan joko haastaa implementoitavaa strategiaa tai seurata, miten strategian toteuttaminen onnistuu. Näin seurataan tietoturvastrategian onnistumista Ylisirniön (2011) esittelemän viitekehyksen mukaisesti.

Kun tietoturvallisuuteen liittyvät tavoitteet ja prosessit on implementoitu ja niiden suorituskyky saatu tavoitellulle tasolle, siirrytään operatiiviseen mittaamiseen ja osoittamaan miten hyvin implementoinnit on loppujen lopuksi onnistuneet ja miten ne ovat paranta-

neet tietoturvallisuutta (Chew et al. 2007; Lippmann et al. 2012). Chew et al. (2007) näkevät tämän tason mittarit taloudellisia vaikutuksia kuvaavina mittareina. Toisaalta ne tarjoavat mahdollisuuden mitata miten luottamusta arvoketjussa on onnistuttu kasvattamaan ja mitä muita vaikutuksia tietoturvallisuuden kehittämisellä on ollut. Lippman et al. (2012) taas näkevät korkeimman maturiteettitason mittarit enemmän riskienhallinnan ja jatkuvan kehittymisen mittareina. Chew et al. (2007) huomioivat, että eri maturiteettitason mittareita voi olla samaan aikaan käytössä. Toisin sanoen kuvassa 4.2 ei ole esitetty aikadimensiota, vaan se ilmaisee sen, että tietoturvallisuuden tason parantuessa käytetään kehittyneempiä mittareita. On myös huomioitava, että alimman tason kehittymistä seuraavien mittareiden avulla on mahdollista kehittää tietoturvallisuutta. Lippmannin et al. (2012) mukaan tietoturvallisuus paranee eniten, kun siirrytään käyttämään operatiivisia mittareita. Chew et al. (2007) eivät ota tähän kantaa.

On huomioitava, että edellä esitetty maturiteettitasoon liitetty mittariston kehitysprojekti ei perustu tieteellisiin lähteisiin. Tietoturvallisuuden mittauksen osalta on kuitenkin perusteltua pohtia, miten mittaamisen voisi aloittaa ja mitä kypsien mittareiden kehitys vaatii, sillä käytännössä toimivia mittareita ei ole onnistuttu implementoimaan. Aiheesta ei löydy tieteellistä tutkimusta, vaan maturiteettitasoista puhutaan usein esimerkiksi konsulttiyritysten julkaisuissa tai osana standardeja. Strategian, järjestelmäkehityksen ja yleisesti organisaation toiminnan suunnitelmallisuuden yhteydessä kuitenkin puhutaan usein maturiteetista. Ylisirniö (2011) huomioi maturiteetin strategian suunnitelmallisuudessa ja siinä, kuinka hyvin ja aktiivisesti sitä jalkautetaan osaksi operatiivista toimintaa. Paulk et al. (1993) taas huomioivat maturiteetin osana tietojärjestelmiä, niiden kehittämistä ja niihin liittyviä projekteja. Yleisesti voidaan sanoa, että mitä paremmin organisaation prosessit on mallinnettu ja johdettu sitä paremmalla maturiteetti tasolla organisaatio on. Kyky mitata prosesseja liittyy usein korkeaan maturiteettitasoon, mutta kuvan 4.2 mukaisesti mittareilla voidaan tukea myös mittauksen kohteen tason parantumista.

Tietoturvamittarien kehittäminen voidaan nähdä samanlaisena prosessina kuin muidenkin mittareiden suunnittelu. Tosin mittaamistapa ja mittaamisen tavoitteet vaihtelevat vahvasti sen mukaan, kuinka hyvällä maturiteettitasolla organisaation tietoturvallisuuden hallinnointi on. Datta & Benerjee (2011) sekä Barabanov et al. (2011) esittelevät standardiin perustuvan viitekehyksen tietoturvamittareiden kehittämiselle. Heidän mukaansa tietoturvamittareiden kehitysprojekti on vahvasti sidottu tietoturvallisuuden maturiteetti tasoihin, jotka esiteltiin kuvassa 4.2. Kuvassa 4.3 on esitetty tietoturvamittareiden kehitysprojekti.



Kuva 4.3. *Mittariston kehittäminen. (Mukailtu lähteistä Datta & Banerjee 2011; Barabanov et al. 2011)*

Kuten kuvasta 4.3 huomataan, mittariston kehittäminen aloitetaan tietoturvallisuuden hallinnan ja siihen liittyvien toimenpiteiden suunnittelulla, jonka jälkeen mitataan miten suunnitellut projektit etenevät. Tämä ilmenee siitä, että ensimmäiset vaiheet ovat hyvin samankaltaiset tietoturvastrategian käytäntöön viemisen prosessin vaiheet. Mittariston kehityssuunnitelma siis olettaa, että organisaation tietoturvallisuus on matalalla maturiteettitasolla ja yksi tavoitteista on sitä kehittää. Toisaalta kehityssuunnitelma sopii hyvin myös yksittäisten toimintojen kehittämiseen ja mittaamiseen kuin osaksi tietoturvastrategian jalkauttamista käytännön toimintaan. Kuvassa 4.3 ei huomioida sitä, miten mittariston suunnittelu käytännössä toteutetaan. Tätä aihetta käsiteltiin kuvassa 3.5, jossa esiteltiin suorituskyvyn mittaamisen päävaiheet. Käytännössä luvussa 3.4 esitelty mittareiden suunnittelu tulisi tehdä aina ennen kehitysprojektin, sen tulosten ja sen vaikutusten mittaamista.

5 TUTKIMUKSEN KOHDE, MENETELMÄT JA TOTEUTUS

Tässä luvussa esitellään kohdeyritys ja tutkimusmenetelmät, joita käytetään tutkimuksen empiirisessä osuudessa. Pääasiallinen tutkimusmenetelmä on toimintatutkimus, jonka tukena käytetään teemahaastattelua ja avointa haastattelua. Lisäksi tässä luvussa esitellään toimintatutkimuksen tueksi teemahaastatteluilla kerätyn aineiston analyysimenetelmä ja kuvaillaan, miten toimintatutkimuksena toteutettu mittariston kehitysprojekti on toteutettu. Näiden asioiden taustaksi kuvaillaan tutkimuksen kohteena olevaa yritystä tutkimukselle relevantista näkökulmasta.

5.1 Kohdeyritys ja mittaristoprojekti

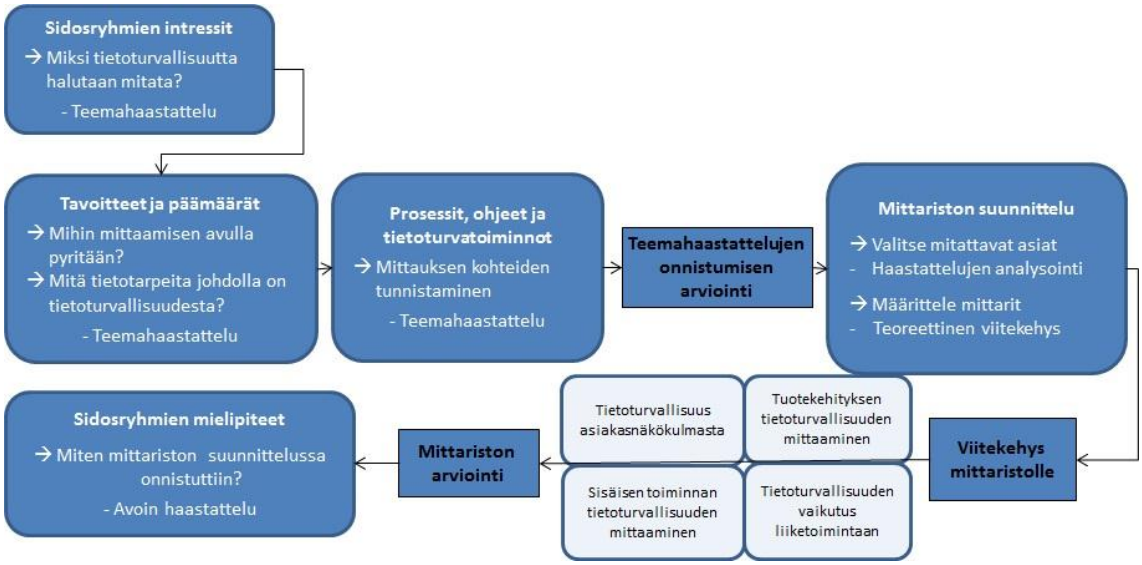
Tutkimuksen kohdeyrityksenä on keskisuuri suomalainen pörssiyhtiö, jolla on halukuutta selvittää, minkälainen mittaristo voidaan kehittää tukemaan tietoturvapäällikön työtä, tietoturvan kokonaisuuden hallinnan ja asiakasvaatimusten paremman hahmottamisen vuoksi. Yritys tuottaa palveluja ja tuotteita globaaleilla markkinoilla laajalle asiakaskunnalle. Tutkimukseen jouduttiin etsimään Nixu Oy:n ulkopuolinen yritys, sillä tutkimuksen kautta haluttiin ymmärtää miten mahdolliset asiakkaat näkevät aihepiirin. Kohdeyritys ei näin ollen ole sitoutunut käyttöönottamaan tai edelleen kehittämään mittaristoa tämän tutkimuksen tuloksena, vaikka vahvaa kiinnostusta mittaamiseen tutkimuksen aikana havaittiinkin.

Tutkimuksen kannalta tärkeitä asioita yrityksen toiminnassa on muutamia. Ensinnäkin yritys ei ole keskusohjattu, eli yritys ei pyri tarkastamalla ja valvomalla kontrolloimaan henkilöstön toimintaa. Tämän sijaan yritys asettaa tavoitteita ja vastuita henkilöstölle ja pyrkii varmistamaan, että oikea osaaminen on oikeassa paikassa. Kohdeyrityksessä ei siis ole kulttuuria, joka tukisi mittaamista. Kaiken kaikkiaan kohdeyritys on haastateltujen mukaan huono mittaamaan, eikä se ole esimerkiksi muodostanut täysin formaalia mittaristoa johdon käytettäväksi tai raportoinnin tueksi. Lähtökohtaisesti kohdeyrityksen edustajia haastattelemalla pyritään selvittämään, mitä tietoturvallisuuden mittaaminen kohdeyrityksessä voisi tarkoittaa. Näin ollen kohdeyrityksellä ei ole vaatimuksia mittareiden hienosäädölle tai esimerkiksi visualisoinnille, vaan motivaatiotekijänä on ymmärtää mitä tietoturvallisuuden mittaaminen tarkoittaa liiketoiminnan näkökulmasta.

Toinen tutkimukseen vaikuttava seikka on tietoturvallisuusyksikön organisatorinen asema. Tietoturvallisuus on kohdeyrityksessä IT-yksikön alla tukifunktiona. Käytännös-

sä tietoturvallisuus on yrityksen sisäinen konsulttitalo, jota hyödynnetään tarvittaessa. Tietoturvayksikölle ei ole asetettu yrityksen laajuista tavoitetta. Tämä tekee osaltaan tietoturvapäällikön työstä reaktiivista. Tietoturvallisuudesta raportoidaan johdolle jokseenkin epämuodollisesti, mutta siihen ollaan kehittämässä formaaleja käytäntöjä. Myös tähän tarpeeseen tutkimuksen tuloksista on hyötyä, sillä mittareiden avulla raporttien sisällön informatiivisuutta voidaan kehittää. Kartoitus siitä, mikä ylintä johtoa kiinnostaa tietoturvallisuuden kannalta, tukee myös osaltaan tietoturvaraportointia.

Mittaristoprojektia varten tähän tutkimukseen koostettiin kattava teoria, jossa tunnistettiin mittariston kehittämiseen ja suunnitteluun liittyviä asioita. Lisäksi laajan teoriaosuuden perusteena oli muodostaa tutkijalle ymmärrys tietoturvallisuudesta ja mittaamisesta. Kohdeyritys valikoitui tutkimuksen empiirisen osion tutkimuksen kohteeksi, koska se kartoittaa mahdollisuuksia mitata tietoturvallisuuttaan. Tämä tutkimus on siis osaltaan esiselvitys laajemmalle mittaristoprojektille. Empiirinen osio jakautui neljään osioon, jotka toteutettiin teemahaastelun, haastattelujen analysoinnin, teoreettisen viitekehyksen ja lopulta avoimen haastattelun avulla. Kuvassa 5.1 esitellään tutkimuksen empiirisen osion kulku, eli käytännössä toteutettu mittaristoprojekti. Mittaristoprojektin suunnitteluun hyödynnettiin luvussa 3.4 esiteltyä suorituskyvyn mittaamisen prosessia, jossa löydettiin mittariston suunnitteluun vaikuttavia tekijöitä. Luvussa 4.5 esiteltyä mittariston kehitysprojektia taas hyödynnettiin kokonaisuudessa siten, että sen kautta löydettiin rakenne empiirisen osuuden tutkimukselle. On myös huomattava, että empiirisen osuuden toteutustapa vastaa hyvinkin paljon kuvassa 2.2 esiteltyä tietoturvallisuuden strategian jalkauttamiseen liittyviä tasoja.



Kuva 5.1. *Tutkimuksen empiirisen osuuden toteutustapa: Mittariston kehitysprojekti*

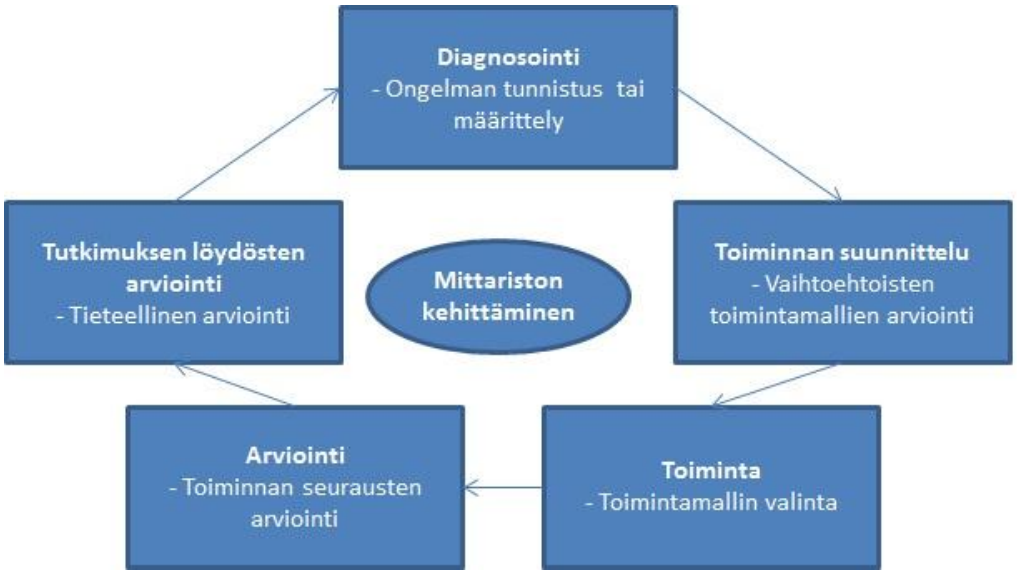
Kuvasta 5.1 ilmenee, että tutkimuksen osiot muodostavat kokonaisuudessaan toimintatutkimuksen, joka on tämän tutkimuksen pääasiallinen tutkimusmenetelmä. Käsiteanalyyttisen teoriaosuuden avulla muodostettiin tutkijan ymmärrys aihepiiristä sekä

löydettiin viitekehys, jonka avulla empiirinen osio pystyttiin toteuttamaan. Myös kohdeyrityksessä käydyt teemahaastattelut ja haastattelujen analysointi auttoivat osaltaan mittarien määrittelyssä, mutta ennen kaikkea niiden avulla pystyttiin löytämään mittauksen kohteet ja perustelemaan syitä mittaamiselle. Tässä tutkimuksessa käytetyt tutkimusmenetelmät esitellään seuraavissa luvuissa.

5.2 Mittaristoprojektin toteutus toimintatutkimuksena

Tässä tutkimuksessa mittaamista ja tietoturvallisuutta tarkastellaan johtamisen kannalta liiketoimintaympäristössä toimintatutkimuksen menetelmin. Toimintatutkimuksissa tutkijan rooli on kaksijakoinen. Toisaalta tutkija pyrkii tekemään tieteellisesti relevantin tutkimuksen, jossa perehdytään aihepiirin aikaisempaan tutkimukseen ja pyritään vertailemaan tutkimuksen löydöksiä niihin. Toisaalta tutkija ottaa konsultin roolin, jossa hän pyrkii vaikuttamaan tutkimuksen kohteeseen ja edesauttamaan muutosta. Toimintatutkimuksessa tutkijan tulee olla läheisessä yhteistyössä tutkimuksen kohteena olevan yrityksen henkilöstön kanssa, jotta tutkija pystyy muodostamaan holistisen kuvan tutkimusongelmasta. Tutkimusongelmaa voidaan lähestyä myös muiden tutkimusmenetelmien avulla. Toimintatutkimusta varten tutkijalla tulee olla riittävät esitiedot aihealueesta, sillä tutkijan osaaminen ja asiantuntevuus ovat merkittävä menestystekijä tutkimuksen onnistumiselle. (Gummesson 2000, s. 119-121)

Susmanin & Everdin (1978) mukaan toimintatutkimus koostuu viidestä vaiheesta, joiden avulla pyritään kehittämään kohdeyritykselle sopiva lopputulos, tässä tutkimuksessa tietoturvamittaristo, ja ratkaisemaan tutkimusongelma. Ensimmäinen vaihe on diagnosointi, jossa tunnistetaan ratkaistava ongelma ja määritellään se tarkemmin. Toimintatutkimuksen toisessa vaiheessa suunnitellaan, miten ongelmaa lähdetään ratkaisemaan. Tämän jälkeen voidaan siirtyä itse toimintaan, jonka tukena käytetään suunniteltua toimintamallia. Kun toimintamalli on viety käytäntöön, toimintatutkimuksen neljännessä vaiheessa arvioidaan, miten toiminta on vaikuttanut kohdeyritykseen. (Susman & Everd 1978.) Toimintatutkimuksen lopuksi on tulee tarkastella yleisiä löydöksiä ja arvioida, miten tutkimuksen tulokset suhtautuvat olemassa oleviin teorioihin ja kirjallisuuteen (Susman & Everd 1978; Gummesson 2000, s. 214-215). Kuvassa 5.2 esitellään toimintatutkimuksen prosessi.



Kuva 5.2. Toimintatutkimuksen prosessi. (Mukailtu lähteestä Susman & Everd 1978)

Tämän tutkimuksen voidaan nähdä sijoittuvan toimintatutkimuksen prosessin eri vaiheisiin. Tutkimuksen lähtökohdan muodosti tutkimusongelma, jonka perustella lähdettiin selvittämään mitä tietoturvallisuus ja mittaaminen tarkoittavat johtamisen näkökulmasta. Teoriaosuuden voidaan kokonaisuudessaan nähdä tarkoittavan ongelman tunnistamista ja sen määrittelyä tukevaa toimintaa. Kirjallisuuden avulla määriteltiin muun muassa yleisesti tunnetut haasteet tietoturvallisuuden mittaamiseksi ja tunnistettiin miten mittaamista voidaan hyödyntää johtamisen tukena. Varsinainen diagnosointi vaihe toteutettiin kuitenkin vasta teemahaastattelujen avulla, joilla kerättiin mittariston suunnittelua varten taustatietoa. Teemahaastatteluista saadun aineiston perusteella määriteltiin syitä mittaamisella ja tunnistettiin tietoturvallisuuteen liittyviä tietotarpeita.

Diagnosointivaiheessa saatua aineistoa analysoitiin aineistolähtöisen sisällönanalyysin keinoin. Haastattelut ja aineiston analyysimenetelmä on kuvattu seuraavissa luvuissa. Suunnitteluvaiheessa tietotarpeet jaoteltiin ryhmiin ja niistä etsittiin kokonaisuuksia, jotka kohdeyritys näkee tärkeänä. Näitä asioita vertailtiin teoriaosuudessa tehtyihin löydöksiin. Tutkijan teorian ja haastattelujen perusteella muodostaman ymmärryksen kautta pohdittiin, miten mittaaminen ja mittaristo voitaisiin toteuttaa. Suunnitteluvaiheessa löydettiin vahvasti kaksi erilaista näkökulmaa: sisäinen tietoturvallisuus ja asiakkaan kokema tietoturvallisuus. Tätä kautta muodostui ajatus tasapainotetun tuloskortin käytöstä. Tasapainotetun tuloskortin käyttöä tuki myös aihepiirin kirjallisuus. Esimerkiksi Brotby (2009) mainitsee että tasapainotettu tuloskortti olisi paras keino kuvailla tietoturvallisuutta ja Jaquith (2007) hahmottelee tietoturvamittareita tasapainotetun mittariston viitekehykseen. Haastatteluissa löydettyjen näkökulmien ja kirjallisuudessa tunnistetun viitekehyksen perusteella luokitellusta haastatteluaineistosta etsittiin tasapainotetun mittariston osa-alueisiin sopivia teemoja. Kirjallisuuden avulla taas pohdittiin, miten mittaaminen on mahdollista toteuttaa siten, että se kuvailee haastatteluissa löydettyjä tietotarpeita. Löydetyt mittaamisen syyt ja aihealueet raportoitiin kohdeyritykselle.

Kohdeyrityksen tietoturvapäällikkö tarkasti raportoidut haastattelut ja antoi arvionsa siitä, kuinka kohdeyrityksen tietoturvallisuuden tila ja sen erityispiirteet oli ymmärretty. Positiivisen arvion perusteella voitiin siirtyä toimintavaiheeseen.

Suunnitteluvaiheen avulla löydettiin siis toimintamalli mittaamiselle ja siihen liittyvät mittauksen kohteet, joiden perusteella mittaristo toteutettiin toimintavaiheessa. Toteutusta ohjasivat vahvasti haastateltujen näkemykset siitä, mitä mitattaisiin. Viitekehyksen rakentamista taas tuki teoriaosuudessa esitellyn tasapainotetun tuloskortin taustalla oleva ajatus siitä, miten oppimisen näkökulma vaikuttaa sisäiseen toimintaan, jolla vaikutetaan asiakasnäkökulmaan, joka vaikuttaa liikevaihtoon. Mittariston toteutusta lähdettiin hahmottelemaan asiakasnäkökulman kautta, jonka jälkeen pohdittiin miten sisäinen näkökulma siihen vaikuttaa. Koska sisäinen toiminta vaikuttaa asiakkaan kokemaan tietoturvallisuuteen sekä sisäisten ongelmien että tuotteiden ja palveluiden tietoturvallisuuden kautta, päätettiin oppimiseen liittyvät mittarit sisällyttää näihin teemoihin. Toimintamalliin lisättiin liiketoiminnan näkökulma ja siihen liittyvät mittarit, joihin muiden teemojen mittareita voidaan yhdistää.

Muodostettu viitekehys mittaristolle raportoitiin toimintavaiheen lopuksi kohdeyritykselle. Raportin perusteella kohdeyrityksen avainhenkilöt arvioivat mittareiden hyvyyttä, niiden soveltuvuutta organisaation käyttöön sekä kykyä tukea päätöksentekoa ja tietoturvallisuuden hallinnointia. Toimintatutkimuksen löydösten tieteellinen arviointi taas suoritettiin kirjallisuudesta löydettyjen kriteerien avulla. Kriteerejä esiteltiin luvussa 3.4. Tämän lisäksi toimintatutkimusta arvioitiin kokonaisuudessa tieteellisestä näkökulmasta, jotta voitiin varmistua onko lopputulokset muodostettu siten, että ne voidaan yleistää sopivan myös tämän tapaustutkimuksen ulkopuolisiin tapauksiin.

5.3 Haastattelut toimintatutkimuksen tukena

Erilaiset haastattelumenetelmät voidaan jakaa kolmeen pääryhmään sen mukaan, kuinka vahvasti haastattelija ohjaa haastattelun kulkua, kysymysten asettelua ja miten kysymykset asetellaan. Täysin strukturoitu haastattelu viittaa haastatteluun, jossa tutkija esittää etukäteen valmistellut kysymykset ja antaa haastattelijalle vastausvaihtoehdot. Strukturoitua haastattelua kutsutaan usein myös lomakehaastatteluksi, jossa tutkija on etukäteen valmistellut kysymykset tiettyyn järjestykseen ja antaa haastateltavalle vastausvaihtoehdot. Täysin strukturoimaton haastattelu pyrkii minimoimaan tutkijan vaikutuksen haastattelutilanteeseen, jolloin haastattelun kohde voi nostaa haastatteluun asioita, joita tutkija ei ollut etukäteen huomioinut. Strukturoimatonta haastattelua voidaan kutsua avoimeksi haastatteluksi, sillä tutkijalla on vain yleinen mielenkiinnon aihe, josta haastateltavan kanssa keskustellaan. Haastateltava vastaa omin sanoin kysymyksiin ja hän voi ohjata haastattelua haluamaansa suuntaan. (Koskinen et al. 2005, s. 104-105, 108)

Tässä tutkimuksessa mittaristoprosessin tueksi on kerätty tietoa hyödyntämällä puolistrukturoitua haastattelua, eli teemahaastattelua. Teemahaastattelu sijoittuu edellä esitettyjen haastattelumuotojen välimaastoon. Teemahaastattelu perustuu eri teemojen läpikäyntiin haastattelutilanteessa, jossa tutkija on päättänyt läpikäytävät teemat etukäteen ja rakentanut niiden pohjalta haastattelurungon. Strukturoitua haastattelua mukaillen teemahaastattelu etenee kysymysrungon mukaisesti, mutta se ei ole ehdoton edellytys. Olennainen ero strukturoituun haastatteluun on haastattelijan vapaus poiketa haastattelurungosta ja esittää lisäkysymyksiä uusien ajatusten herättämiseksi. Haastattelurunko taas erottaa teemahaastattelun strukturoimattomasta haastattelusta, mutta myös teemahaastattelussa tutkija voi antaa tilaa ja aikaa haastateltavan tulkinnoille, pohdinnoille ja analyyseille. Näin voidaan syventyä aihealueeseen ja ymmärtää laajemmin haastateltavan näkemyksiä. (Koskinen et al. 2005, 104-105, 108)

Teemahaastattelun käyttö sopii hyvin toimintatutkimuksen tueksi. Sekä toimintatutkimuksessa että mittaamista tutkittaessa on keskeistä saavuttaa ymmärrys kohdeyrityksen toiminnasta. Mittauksen kannalta on tärkeää ymmärtää miksi mitataan ja mitä mitataan ennen kun voidaan antaa suosituksia siitä miten mitattaisiin. Jotta näihin kysymyksiin saataisiin vastauksia, haastattelut vaativat kysymysrungon. Toisaalta teemahaastattelun mahdollistamien lisäkysymysten avulla voidaan tarkentaa haastateltavien perusteluja ja mielipiteitä tietoturvallisuuden mittaamisesta, jolloin tutkimuksen kohdetta voidaan ymmärtää syvällisemmin kuin ennakkoon suunniteltujen kysymysten kautta. Teemahaastattelut suoritettiin kohdeyrityksen tiloissa syyskuussa 2012. Haastattelutilanteissa olivat mukana vain tutkija ja haastateltava. Kahdeksan haastatellun taustat esitellään seuraavassa luvussa.

Liitteessä 1 on esitetty haastattelurunko, jota käytettiin teemahaastattelujen tukena. Haastattelu kysymykset pyrittiin käymään läpi rungossa esitetyssä järjestyksessä, mutta usein haastattelutilanteessa päädyttiin hieman erilaiseen järjestetykseen. Haastattelurungon alkupään kysymysten avulla pyrittiin ymmärtämään haastateltavien suhtautumista tietoturvallisuuteen ja sitä, miten tietoturvallisuus vaikuttaa heidän työn tekemiseen ja päätöksentekoon. Näin selvitettiin käyttötapauksia tietoturvamittareille. Tämän jälkeen haastattelurungossa käytiin läpi tutkimuksen haastatteluteemat. Haastatteluteemat muodostettiin tutkimuskysymysten perusteella ja kysymysten avulla pyrittiin löytämään liiketoiminnan näkökulma tietoturvallisuuteen. Tästä syystä haastatelluilta kysyttiin pikemminkin tavoitteita tietoturvallisuudelle sekä kannustettiin pohtimaan tiedon aiheuttamia uhkia liiketoiminnalle sen sijaan että olisi kysytty suoraan tietoturvallisuudesta. Teemoihin etsittiin vastauksia, joiden avulla tietoturvallisuus pystyttiin ymmärtämään osana liiketoimintaprosesseja sekä raportointia.

Myös avoin haastattelu sopii toimintatutkimuksen tueksi, sillä tulosten kattavaa arviointia varten haastateltavia ei voi johdatella liikaa ja heille tulee antaa mahdollisuus kertoa mielipiteensä avoimesti. Avoin haastattelu sopii hyvin myös mittariston arviointiin, sillä

avoimessa haastattelussa kohdeyrityksen edustajat pystyvät vapaasti kommentoimaan mittaristoa ja huomiomaan asioita, jotka tutkijalta oli mahdollisesti jäänyt huomioimatta. Tässä tutkimuksessa avoin haastattelu toteutettiin sähköpostitse. Teemahaastatteluihin osallistuneille lähettiin kuvaus mittaristosta ja pyyntö arvioida sen soveltuvuutta kohdeyritykselle. Vapaamuotoiset vastaukset vastaanotettiin sähköpostitse ja niiden perusteella kirjoitettiin tietoturvamittariston arviointi kohdeyrityksen näkökulmasta. Avoimen haastattelun ongelmaksi muodostui, että vain kolme teemahaastatteluun osallistunutta, tietoturvapäällikkö, asiantuntija ja johtaja, vastasivat arviointipyyntöön.

5.3.1 Haastateltavien taustat ja suhde tietoturvallisuuteen

Työnkuvan suhteen haastateltavien painopiste on liiketoimintaa johtavissa henkilöissä. Kolme haastateltua ovat johtoryhmän jäseniä ja kolme ovat eri liiketoimintalinjojen johtajia. Lisäksi mukana tutkimuksessa on tietoturvapäällikkö ja asiantuntija, joilla on syvällinen käsitys kohdeyrityksen tietoturvallisuudesta. Jokaisen haastatellun vastaukset on käsitelty samalla tavalla liiketoiminnan näkökulmasta, mutta asiantuntijan haastattelu painottui tietoturvallisuuslähtöisyyteen. Jaottelu liiketoiminnasta ja tietoturvallisuudesta vastaavien henkilöiden suhteen on tutkimuksen kannalta mielenkiintoista, sillä sisäisestä tietoturvallisuuden toteutuksesta saadaan laaja-alainen kuva. Tämän lisäksi voidaan löytää eroja tietotarpeissa ja tutkia mahdollisuuksia liittää tietoturvallisuus osaksi liiketoimintaprosesseja, kun haastatteluista saatuja tuloksia tutkitaan yhdessä ja vertaillaan toisiinsa. Tutkimuksen kannalta nämä asiat tukevat tavoitetta löytää keinoja kuvailla tietoturvallisuuden tilaa mittareiden avulla. Haastateltavien taustatiedot on esitetty taulukossa 5.1.

Taulukko 5.1. *Haastateltavien taustatiedot.*

	Työnkuva	Tuntee yrityksen tietoturvallisuuden ja sen hallintakeinot asteikolla 1-5 (1=huono, 5=erinomainen)	Arvio kohdeyrityksen tietoturvallisuuden tilasta 1-10 (1 = huono, 10=erinomainen	Vaikuttaako tietoturvallisuus päätöksentekoon / Pitäisikö tietoturvallisuutta mitata
Hlö 1	Johtoryhmän jäsen	4	8	Kyllä / Kyllä, jotta tiedettäisiin että ollaan hyviä muttei kalliita
Hlö 2	Johtoryhmän jäsen	2	6,5	Kyllä / Kyllä, jos se liitetään liiketoimintakontekstiin
Hlö 3	Johtoryhmän jäsen	4	8,5	Kyllä / Kyllä, prosessin mittaamisen osana
Hlö 4	Johtaja	4,5	6,5	Kyllä / Kyllä, koska tarvitaan holistinen näkymä tietoturvan tilasta
Hlö 5	Johtaja	4	8,5	Kyllä / Kyllä, jotta olisi käsitys siitä missä ollaan
Hlö 6	Johtaja	2	3	Kyllä / Kyllä, jotta voitaisiin määrittää hyväksyttävä taso ja siihen liittyvät tavoitteet
Hlö 7	Tietoturvapäällikkö	5	5	Kyllä / Kyllä, koska mittaamalla voidaan vaikuttaa toimintaan
Hlö 8	Asiantuntija	3	8	Kyllä / Kyllä, jos on resursseja hyödyntää tuloksia muutoksen toteutuksessa

Haastateltujen työkokemus kohdeyrityksessä vaihtelee yhden ja yli kymmenen vuoden välillä. Tälle ei ole tutkimukseen liittyvää perustetta, vaan haastatellut pyrittiin valitsemaan ensinnäkin mahdollisimman korkeasta organisatorisesta roolista ja toisaalta siitä yhtä tasoa alempaa liiketoimintalinjojen johdosta. Vain yhden vuoden työssä olleiden haastatteleminen oli perusteltua, sillä heidän aikaisempi kokemus tietoturvasta oli riittävän hyvä, sekä heidän näkemyksensä kohdeyrityksen tietoturvallisuudesta olivat kohtalaisen tuoreita. Näistä lähtökohdista saatiin käsitys liiketoiminnallisen johdon näkökulmasta kohdeyrityksen tietoturvallisuuden suhteen, jota pystyttiin syventämään tietoturva-asiantuntijoiden näkemyksellä. Alempia organisatorisia rooleja ei haastateltu, sillä tutkimuksella pyrittiin löytämään tekijöitä, joiden avulla organisaation tietoturvallisuuden tilaa voidaan kuvailla ylimmälle johdolle ja toisaalta keinoja, joilla tietoturvapäällikkö voi viestiä tietoturvan tilasta holistisesti. On myös huomioitava, että tämän tutkimuksen laajuudessa koko yrityksen toimintaa ei voitu käydä läpi tai haastatella jokaista johtotasoa läpi. Tämän tutkimuksen puitteissa pyrittiin siis löytämään, mikä kokonaisuudessaan on yritykselle tärkeää tietoturvallisuuden näkökulmasta.

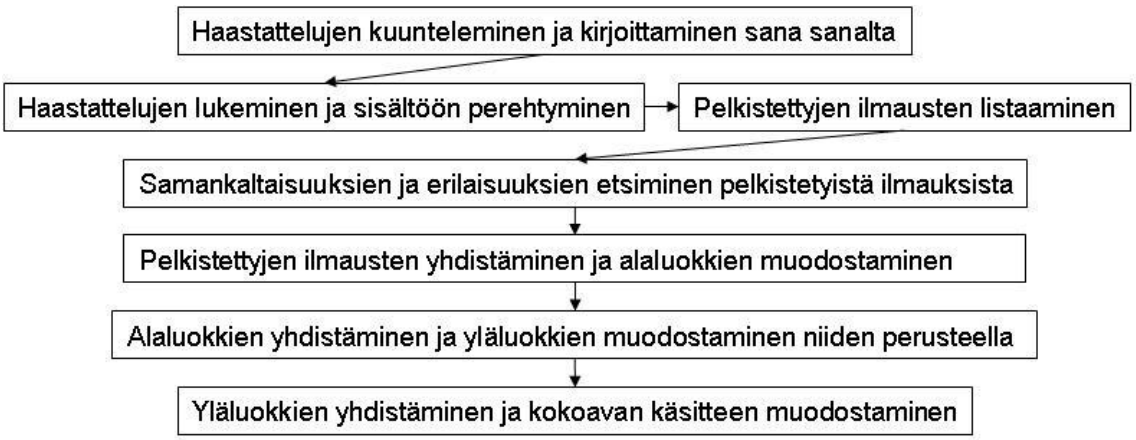
Kaksi haastatelluista arvioi tuntevansa kohdeyrityksen tietoturvallisuuden ja sen hallintakeinot heikosti. Heidän haastatteleminen oli kuitenkin perusteltua, sillä heidän tietämys tietoturvallisuuteen liittyvistä vaatimuksista, joita kohdeyritykselle tulee kolmansilta osapuolilta, oli vahva. Molemmat ilmaisivat tuntevansa kohdeyritykset tietoturvallisuuden erinomaisesti vaatimusten näkökulmasta, mutta heiltä puuttui näkemys tietoturvallisuuden tilasta ja käytännön toteutuksesta. Viisi haastateltua ilmaisi tuntevansa kohdeyrityksen tietoturvallisuuden ja sen hallintakeinot erittäin hyvin, joten heidän haastatteleminen oli todella relevanttia. Liki kaikkien haastateltujen arvio tietoturvallisuuden tilasta vaihteli kohtalaisen ja hyvän välillä. Huonoimman arvion antanut johtaja sanoi suhtautuvansa kriittisesti havaitsemiinsa epäkohtiin, jotka vaikuttivat vahvasti hänen mielipiteeseen. Tietoturvapäällikön mielipide, keskiverto tietoturvan tila, taas kuvastaa sitä, että hän näkee päivittäisessä työssään kaikki tietoturvallisuuteen liittyvät ongelmat ja kehittämiskohteet.

Jokainen haastateltava kertoi tietoturvallisuuden vaikuttavan heidän päätöksentekoon. Tähän yleinen syy oli asiakasvaatimukset, mutta myös huoli henkilökohtaisten laitteiden käytön turvallisuudesta ja yleisesti tietoturvauhat. Tähän liittyen haastateltavilta kysyttiin, pitäisikö tietoturvallisuutta mitata. Jokainen haastatelluista vastasi tähän positiivisesti, joten tutkimus oli aiheellista suorittaa. Kolme haastateltavaa asetti kuitenkin reunaehdon. Yhden johtoryhmän jäsenen mukaan mittaaminen olisi relevanttia osana prosessien mittaamista ja toinen arvioi, että tietoturvallisuutta voisi mitata yleisemmin osana laadun mittaamista. Tietoturva-asiantuntijan mukaan mittaaminen on turhaa, ellei sen tulosten avulla voida tehdä muutoksia toiminnassa. Tämä argumentti toimii myös perusteeksi sille, että tutkimuksessa haastateltiin korkean tason johtajia.

Tietoturvallisuuden tila tarkoittaa haastateltaville niiden asioiden suorittamista, jotka määritellään asiakasvaatimuksissa ja jotka viedään eteenpäin muille kolmansille osapuolille. Toisaalta yksi johtoryhmän jäsen kuvaili, että mitä kypsempiä prosessit ovat, sen parempi on myös niiden tietoturvallisuuden tila. Kohdeyrityksen tietoturvallisuuden tila muodostuu siis vaatimusten ja niiden soveltamisen kautta. Tähän liittyy tietoturvallisuuden perusasiat, kuten tekninen tietoturvallisuus, pääsynvalvonta, fyysinen turvallisuus ja tietoturvaosaamisen taso. Tietoturvallisuuden tilaa heikentää toteuttamattomat kehitysprojektit, huono näkyvyys tietoturvallisuudesta kokonaisuutena sekä se, että usein panostetaan liikaa siihen, miltä tuote näyttää huomioimatta sitä, mikä sen takana olevien järjestelmien taso on. Muutaman haastateltavan mukaan todella hyvä tietoturvallisuuden tila olisi sellainen, että voidaan osoittaa oman toiminnan laadukkuus asiakkaalle, jolloin asiakasvaatimusten seuraamiselta vältyttäisiin.

5.3.2 Aineiston analyysimenetelmä

Teemahaastattelut nauhoitettiin ja nauhoitettua aineistoa analysoitiin soveltaen laadullista aineistolähtöistä sisällönanalyysiä, jolloin vastauksista pystyttiin muodostamaan yleistävä kokonaisuus. Haastattelut kuunneltiin läpi ja haastattelujen sisältö kirjoitettiin muistiin. Tavoitteena oli muodostaa käsitys tietoturvallisuuden mittaamisen syistä ja kohteista organisaatiossa ja saada selville, mitkä asiat nousevat vastauksista useimmin esille. Aineistolähtöisen sisällönanalyysin eteneminen on esitetty kuvassa 3.



Kuva 5.1. *Aineistolähtöinen sisällönanalyysi. (Mukailtu lähteestä Tuomi & Sarajärvi 2009, s. 109)*

Muistiinpanoja luettaessa haastattelujen sisältöä käsiteltiin ensin teemoittain, jonka jälkeen pyrittiin löytämään alaluokkia niistä asioista, joita haastateltavat toivat esille. Alaluokkien muodostamisessa kaikkien haastateltavien näkemykset kerättiin Excel-taulukoihin haastattelujen teemojen mukaisesti ja niitä yhdisteltiin kokonaisuuksiksi. Tämän jälkeen teemoihin muodostettiin yläluokkia, joihin alaluokkien sisällöt liitettiin. Johtoryhmän jäsenten näkemyksellä oli suuri merkitys yläluokkia muodostettaessa, kun

taas alaluokkia kuvaavien asioiden suhteen operatiivisemmalla johdolla ja tietoturva-asiantuntijoilla oli paljon näkemyksiä.

Lopuksi yläluokkien suhteet toisiinsa pyrittiin ymmärtämään ja näkemään, mitkä alaluokat ovat tärkeimpiä kohdeyrityksen tietoturvallisuuden kannalta. Näitä alaluokkia, esimerkiksi tietoturvatapahtumia, kuvaavien asioiden avulla muodostettiin lopulta mittareita, joiden avulla alaluokkien tietoturvallisuuden tilaa on mahdollista kuvailla. Yläluokat, esimerkiksi sisäinen tietoturvallisuus, kokonaisuudessaan pyrkivät kuvaamaan kohdeyrityksen tietoturvallisuuden tilaa. Seuraavassa luvussa tutkimuksen tulokset esitellään teemoittain, joista jokainen on jaoteltu yhdenmukaisiin yläluokkiin. Yläluokkia kuvastavat otsikot, joiden alla on käsitelty niitä kuvailevia asioita.

6 TULOKSET

Tutkimuksen teoriaosuudessa tarkasteltiin tietoturvallisuutta ja mittaamista tieteelliseen kirjallisuuteen nojautuen ja muodostettiin teoreettinen viitekehys, jonka pohjalta tutkimuksen aikana kerättyä empiiristä aineistoa on analysoitu. Tässä luvussa esitellään teemahaastatteluiden avulla kerätty tutkimusaineisto ja toimintatutkimuksen toimintavaiheessa muodostettu mittaristo. Teemahaastatteluiden tulokset perustuvat aineistolähtöiseen sisällönanalyysiin ja tutkijalle jääneeseen käsitykseen kohdeyrityksen motivaatiosta mitata tietoturvallisuutta, mittauksen kohteista ja haastateltujen esittämistä keinoista mitata tietoturvallisuutta. Näiden asioiden kautta pystytään hahmottamaan sitä, miten kohdeyrityksen tietoturvallisuuden tilaa voidaan havainnoida ja perustella, miksi se on tärkeää eri osapuolille. Tulosten esittely jakaantuu kolmeen osaan teemahaastattelujen teemojen mukaisesti: miksi tietoturvallisuutta mitataan, mitä tämän mittaamisen osana mitattaisiin ja lopulta miten se käytännössä toteutettaisiin. Nämä teemat jakautuvat vielä neljään yläluokkaan, joiden kautta pyritään muodostamaan kokonaisvaltainen kuvaus tutkimuksen tuloksista.

6.1 Tietotarpeet ja tavoitteet mittaamiselle

Tulosten käsittely ”miksi”-teeman suhteen on jaettu neljään erilliseen yläluokkaan, jotka kaikki pyrkivät tuomaan esiin yhden näkökulman siitä miksi tietoturvallisuutta mitattaisiin. Lisäksi esitellään, mikä on kohdeyrityksen motivaatio mitata eri asioita tietoturvallisuuteen liittyen. Luvussa 3.5 esitellyn mittariston suunnitteluprosessin viitekehyksessä tässä luvussa esitellään lähtökohtia mittaamiselle, eli tunnistetaan tarpeita mittaamiselle. Alaluvut taas on jaoteltu tunnistettujen kehityskohteiden mukaisesti.

Tietoturva-asiantuntija tiivisti ”miksi”-teeman vastauksesi: *”jos sulla on joku idea että mitä sä aiot muuttaa mittausdatan perusteella, sä oot valmis muuttamaan sitä ja sulla on paukut siihen niin sit kannattaa”*. Tässä luvussa etsitään siis perusteluja sille miksi mitattaisiin liiketoimintalähtöisesti. Lähtökohtana voidaan mainita johtoryhmän jäsenen mielipide, että *"tietoturva on hygienia tekijä, sen tulee olla tietyllä tasolla",* joka jo itsessään perustelee johtoryhmän kaipaaman viestin tietoturvallisuudesta, joka mittareiden avulla pystytään viestimään.

6.1.1 Miksi kohdeyrityksen sisäistä toimintaa mitattaisiin?

Sisäisen näkökulman mittaaminen on tärkeää, jotta tietoturvallisuutta osataan kehittää kohti sujuvampaa, asiakkaissa luottamusta herättävää ja liiketoimintaan sidoksissa olevaksi tekijäksi. Eräs johtoryhmän jäsen totesi haastattelussa, että *"Toimiala riippumattomasti se pohdinto pitäisi käydä, että miten se tietoturvallisuus sielä takana"*. Motivaationa mitata tietoturvallisuutta on lähtökohtaisesti se, että mittareiden avulla on mahdollista muodostaa holistinen näkymä siitä, mikä tietoturvallisuuden tila on ja mitkä tekijät siihen vaikuttavat. Lähes kaikki haastatellut toivat tämän näkökulman esille.

Holistinen näkymä tietoturvallisuudesta tarvitaan haastateltujen mukaan myös siksi, ettei tietoturvallisuus olisi liiketoiminnasta irrallinen toiminto. Usea haastateltu mainitsi, että tietoturvallisuutta ei mitata eikä sille ole asetettu tavoitteita. Tästä syystä siitä ei voida viestiä tai sille ei pystytä määrittämään hyväksyttävää tasoa. Koska tietoturvallisuutta ei ole kytketty suoraan mihinkään toimintaan, ei erään johtoryhmän jäsenen mukaan voida nähdä, mihin muutokset vaikuttavat ja mikä on niiden vaikuttavuus. Tietoturvapäällikkö kommentoi lisäksi, että mittaamalla voidaan vaikuttaa toimintaan. Tietotarpeena on kahden johtoryhmän jäsenen mukaan ymmärtää mittaamisen avulla, mikä on relevantti tietoturvallisuuden kannalta.

Tietoturvallisuuden kehittyminen osana prosessien kehittymistä ja koetaan tärkeäksi. Johtoryhmän jäsen perusteli että tietoturvallisuutta tulisi mitata, jotta ymmärretään miten prosessien tietoturvallisuus parantuu niiden kehittyessä. Toinen johtoryhmän jäsen oli kiinnostunut tietämään, mikä omien myytävien tuotteiden ja palveluiden tietoturvantaso on, sekä onko niitä tuottavien prosessien tietoturvallisuus kunnossa. Usea haastateltu mainitsi tähän liittyen tietotarpeeksi sen, että prosessien ja tuotteiden kehityksestä tarvittaisiin mittaustietoa. Mittaustiedon avulla voisi asiantuntijan mukaan pystyä osoittamaan, että sisäisiä asioita tehdään tavoitteen mukaisesti. Useat haastatelluista olivat myös kiinnostuneita tietämään prosessien riskitasosta sekä siitä, miten mittareiden avulla on mahdollista priorisoida riskejä tehokkaammin. Tietoturvapäällikkö huomautti, että mittaustarvetta olisi etenkin niiden prosessien osalta, joissa on havaittu tietoturvaongelmia.

Tietoturvaprosessien mittaaminen nousi esille voimakkaasti tietoturvapäällikön ja asiantuntijan näkökulmasta. Asiantuntija pohti asiaa pikemminkin tuotekehityksen kautta, mutta yleisesti voidaan sanoa että sisäisen toiminnan mittaamisesta on tärkeä eritellä, tietoturvaprosessien mittaaminen. Tätä perusteltiin sillä, että mittaamisen avulla pystyttäisiin hallitsemaan paremmin kaikki tärkeimmät tietoturvaprosessit, eli nähdä missä ollaan hyviä, missä vaaditaan kehityshankkeita ja missä on tapahtunut jotain sellaista mitä ei olisi pitänyt tapahtua. Sekä asiantuntija että tietoturvapäällikkö liittivät tietoturvan kehittämisen vahvasti liiketoiminnan tarpeisiin siitä, mitä on relevanttia kehittää. Myös kaikki johtajat pohtivat, että olisi hyvä ymmärtää erikseen vielä, miten hyvin tie-

toturvaprosesseja noudatetaan. Johtoryhmätasolla tämä ei ollut tärkein teema, vaan tietotarpeena oli yksinkertaisesti se, onko asiat kunnossa vai ei ja jos ei ole, mitä riskejä niistä voi muodostua ja miten ne vaikuttavat laatuun yleisemmällä tasolla.

Kaksi johtoryhmän jäsentä huomio, että henkilökunnan tietoisuus tietoturvasta on tärkeää. Tavoitteena yhden johtajan mukaan on, että tietoturvatietoisuutta koulutettaisiin enemmän. Yksi johtoryhmän jäsen taas ilmaisi, että on tärkeää pitää hyvä osaamistaso kohdeyrityksessä ja varmistaa, että oikeat ihmiset ovat oikeassa paikassa. Koulutus ei kuitenkaan tullut kovin vahvana tietotarpeena esille, vaan lähinnä haluttiin varmistaa, että riittävä osaaminen ja tietämys tietoturvasta ovat olemassa. Esimerkiksi tietoturvapäällikkö huomioi, että kompetenssin mittaaminen vaatisi kalliin investoinnin.

6.1.2 Asiakasnäkökulma osana mittaamista

Asiakasnäkökulma on tärkeä osa tasapainotettua tuloskorttia ja sen avulla määritellään sisäiset prosessit, joissa yrityksen tulee olla tärkeimmillään. Jokainen haastateltava nosti esiin asiakkaisiin liittyvän mittaamiseen. Yksi johtoryhmän jäsenistä tiivisti asiakasnäkökulman mittaamisen tärkeäksi, sillä *"Jos nyt jotain mitataan, niin tietysti sisäinen on aina tärkeetä mutta se pitää nähdä asiakkaan kautta"*. Kohdeyritys haluaa siis mitata tietoturvallisuutensa tasoa asiakkaan näkökulmasta ja siten ymmärtää asiakasta paremmin. Yhden johtoryhmän jäsenen huolenaiheena oli asiakkaiden luottamus siihen, kuinka hyvin kohdeyrityksen taustajärjestelmät pystyvät ylläpitämään palvelua. Toisin sanoen vaikka lopputuote olisi todelle hyvä, näkyy taustajärjestelmien toimimattomuus tai suunnittelemattomat huoltokatkot asiakkaalle palvelukatkoina.

Asiakasvaatimusten täyttämisen tärkeyden mainitsi jokainen haastateltava. Se onkin yksi mittaamisen motivaatiotekijöistä. Kohdeyritys haluaa siis osoittaa, että se toteuttaa asiakasvaatimukset ja toimii niiden mukaisesti aina. Tällä hetkellä tätä ei pystytä todistamaan. Lisäksi asiakasvaatimusten koveneminen aiheuttaa haasteita. Tietoturvapäällikkö huomioi tiukentuneet asiakasvaatimukset ja näki tarpeellisena valuttaa ne läpi organisaation. Asiakasvaatimuksia haluttaisiin siis pystyä mittamaan, jotta johto pystyy helposti näkemään toimitaanko vaatimusten mukaisesti ja nähdä, ymmärretäänkö ne samalla tavalla läpi kohdeyrityksen. Toisaalta eri vaatimuksia haluttiin ymmärtää paremmin ja priorisoida, mitkä niistä pyritään täyttämään. Tietotarpeena nousi esiin, että löydettäisiin heikkoja lenkkejä osana asiakkaan kanssa sovittuja prosesseja ja miten asiakaskohtaamistilanteissa onnistutaan tietoturvallisuuden näkökulmasta. Näitä heikkoja lenkkejä seurataankin jo tällä hetkellä. Muutama haastateltavista totesi, että on tärkeää viedä asiakasvaatimukset eteenpäin toimitusketjussa. Motivaatiota oli siis seurata mittareiden avulla myös toimittajien tietoturvallisuutta.

Suuri motivaatiotekijä asiakasnäkökulman mittaamiseen oli myynnin tukeminen, jonka mainitsi yli puolet haastatelluista. Myynnin tukena halutaan osoittaa, kuinka laadukkaasti ja hyvällä kokemuksella tuotteita tehdään. Tämän avulla tavoitteena olisi pyrkiä

luomaan luotettava kuva asiakkaalle, jonka kautta olisi mahdollista välttyä raskailta asiakasvaatimuksilta tietoturvallisuuden suhteen. Motivaationa mittaamiselle tuli esille, että mittareiden avulla on mahdollista osoittaa asiakkaille *”meidän tapa toimia”*, kuten eräs haastatelluista asian ilmaisi. Toinen haastateltu pohti, että mittareiden tuloksia voisi käyttää myyntiargumenttina. Vaikka näin pitkälle meneviä mittareita ei pystyttäisi muodostamaan, on motivaatiotekijänä tukea myyntiprosessia selkeyttämällä kuvaa omasta toiminnasta suhteessa yleisiin asiakasvaatimuksiin. Eräs haastateltu johtaja totesikin, että myynnin tukena käytettävien mittareiden tuli olla täysin oikeellisia ja yksiselitteisiä, jotta niitä voidaan käyttää osana kaupantekoa.

Muiden kolmansien osapuolten vaatimusten mittaamista ei nähty tärkeänä, eikä esimerkiksi lakiin tai Euroopan Union asettamia vaatimuksia tunnistettu tietoturvallisuuden kannalta sellaisin asioina, joihin mittareita kaivattaisiin laajasti. Esimerkiksi asiantuntija mainitsi, että loppujen lopuksi vaatimuksia ei tule kovinkaan paljon. Kolme haastateltua mainitsi haastattelussa Euroopan Unionin vaatimukset ja yleisesti tiedostettiin, että ne asettavat tiettyjä haasteita kohdeyrityksen toiminnalle. Hieman suurempi tietotarve ilmeni kohdeyrityksen eri toiminta-alueiden riskitason, tietoturvavaatimusten ja ongelmien havaitsemisesta. Lakiin ja säädöksiin liittyvistä tietotarpeista mainitsi kaksi haastateltua johtajaa. Lakeihin liittyvät vaatimukset, esimerkiksi henkilötietoihin liittyen, mainittiin, mutta näitä ei pidetty merkittävinä seikkoina mittaamisen kannalta. Erääksi mittariksi ehdotettiinkin toimintaympäristön aiheuttamien vaatimusten kartoittamista ja niiden vaikutusten arviointia eri toiminta-alueiden liiketoimintavaatimusten näkökulmasta.

6.1.3 Tietoturvallisuuden huomioiminen osana tuotekehitystä

Tietoturvallisuuden huomioiminen osana tuotekehitystä tuli esille sisäisen toiminnan ja tuotteiden kehittämisen kautta. Usea haastateltava pohti mahdollisuutta siihen, että mittareiden avulla mahdollistetaan modulaarisempi ajattelutapa, joka auttaisi tuotekehitystä huomioimaan tietoturvallisuuden. Ajatuksia tähän alaluokkaan tuli kahdella tavalla. Toisaalta asiakasvaatimusten huomioiminen nähtiin tuotekehityksen toiminnan tietotarpeena. Toisin sanoen mittareiden avulla haluttiin sitoa tuotekehitys vahvemmin asiakasvaatimuksiin ja seurata miten näitä toteutetaan. Toinen näkökulma oli päätöksenteon tuki kaikkiin uusiin tuotteisiin ja palveluihin liittyen. Asiantuntija halusi liittää mittaamisen osaksi liiketoiminnan kehityksen tukea, eli että tuotetaan mahdollisimman tietoturvallisia tuotteita. Tämä auttaisi ymmärtämään myytävien tuotteiden tietoturvantasoa, jonka yksi johtaja ja kaksi johtoryhmän jäsentä ilmaisi tietotarpeena. Kaksi johtajaa mainitsi lisäksi, että ne joilla on vastuu tuotteista tarvitsevat tietoa siitä, miten tuotekehitys on huomioinut tietoturvallisuuden.

Yksi johtoryhmän jäsen mainitsi, että kohdeyrityksessä on meneillään neljä laadunparannusprojektia. Johtoryhmän jokainen jäsen ilmaisi haastatteluissa, että tietotarpeena on laatu prosesseihin, tuotteisiin, palveluihin ja niitä ylläpitämiin järjestelmiin liittyen. Tietoturvallisuus taas voidaan nähdä osana laadun kehittämistä, laaturiskejä ja yleisesti

kaikkien asiakkaisiin liittyvien toimintojen laatua. Johtajat näkivät näiden asioiden kehittämisen tuotekehityksen ja itse asetettujen vaatimusten täyttämisen kautta. Tavoitteena mainittiin, että kohdeyritys pystyy itse asettamaan vaatimukset tuotteille, joiden kautta varmistettaisiin hyvä laatu. Tietoturvapäällikön näkökulmasta taas olisi tärkeää nähdä, missä on kehitysprojekteja ja varmistua että tietoturvallisuus huomioidaan niissä, mikäli se on liiketoiminnallisesti relevanttia.

Johtajien ja tietoturvapäällikön mukaan yksi tietoturvallisuuden haaste on, että useita kehitysprojekteja tietoturvallisuuden kehittämiseksi on suunniteltu, mutta näille ei saada riittävää tukea liiketoimintajohdolta. Tietoturvapäällikön mukaan kohdeyrityksessä on prosesseja, jotka eivät tietoturvallisuuden kannalta toimi. Yhden johtajan mukaan *”karu todellisuus on se ettei tehdä niin paljon kun voitas tehdä ja se osin on kiinni siitä ettei me saada resursseja siihen”*. Koska johtoryhmä näkee tietoturvallisuuden vahvasti riskien ja laadun kautta, voidaan mittauksen kohteena pitää tekemättömien asioiden aiheuttamaa riskiä liiketoiminnalle ja niiden vaikutuksia laatuun. Tuotekehityksen ja tietoturvallisuuden kehitysprojektien kautta riskiä pyrittäisiin siis pienentämään ja laatua parantamaan.

6.1.4 Liiketoiminnan tarpeet tietoturvallisuuden mittaamiselle

Lähtökohtana tietoturvallisuuden liittämisenä osaksi liiketoimintaa voidaan pitää erään johtoryhmän jäsenen mielipidettä: *”Tietoturvallisuus ei itsessään ole ollenkaan mielenkiintoista, mutta sitten kun se liittyy johonkin business agendan suorittamiseen niin sitten siinä alkaa olemaan joku paikka ja arvo*”. Tämän jatkona pohdittiin, että niin kauan kun ei ole mittareita, ei tietoturvallisuutta voida liittää osaksi liiketoimintaa ja prosesseja. Tämä näkökulma tuli esille niin johtoryhmätasolla kuin tietoturva-asiantuntijoiden näkemyksissä. Johtoryhmäntasolla tietoturvallisuuden mittaaminen osana liiketoimintaa nähtiin vahvasti riskilähtöisesti. Liiketoimintaprosesseista olisi johtoryhmän näkökulmasta tärkeä tietää, missä on riskejä ja mihin niiden perusteella tulee investoida. Myös johtajien tietotarpeena oli tunnistaa riskejä ja nostaa niitä esiin mittareiden avulla ja ymmärtää tietoturvallisuutta riskien kautta. Tietoturva-asiantuntijat eivät tuoneet tietotarpeita näin voimakkaasti esille riskien kautta, mutta tiedostivat ylemmän johdon tarpeen saada tietoa riskeistä.

Johtoryhmän jäsenen mukaan *"Tietoturvallisuus tulisi ymmärtää end-to-end jotta ymmärrettäisiin miten se liittyy businesskontekstiin eikä sitä käsiteltäisiin irrallisena asiana"*. Tällä tarkoitetaan motivaatiota pohtia, miten tietoturvallisuus näkyy läpi arvoketjun toimittajien, kohdeyrityksen, yhteistyökumppanien ja lopulta asiakkaiden kautta. Tietoturvallisuuden mittaamisesta oltiin motivoituneita, kun pohdittiin sitä miten toimittajat ja yhteistyökumppanit pääsevät kohdeyrityksen järjestelmiin ja ylipäänsä miten ulkopuoliset tahot niihin pääsevät. Toinen tietotarve oli erityisesti liiketoimintakriittisten järjestelmien tietoturvallisuus. Näiden kohdalla kaksi johtoryhmän jäsentä ilmaisi huo-

len siitä, miten tietoturvallisuus ja järjestelmät pystyvät turvaamaan uuden toimintatavan.

Kohdeyrityksen teollisuudessa on tapahtunut iso murros, joka koventaa asiakasvaatimuksia ja tätä kautta asettaa järjestelmille uusia riskejä. Liiketoiminnan motivaatio liittyi usein investointeihin, riskeihin ja asiakkaannäkemykseen, kun taas johto ja asiantuntija tasolla näitä pohdittiin ongelmien ja tietoturvatapahtumien kautta. Johtoryhmälle tärkeää oli myös asiakkaiden maineen säilyttäminen ja tätä kautta kohdeyrityksen hyvän maineen lisääminen. Tosin tietoturvapäällikkö kaipasi mittaustietoa siitä, mikä on jonkin toiminnon liiketoiminta-arvo kun siihen pitäisi investoida. Tietoa voisi verrata siihen, että onko tietoturvatoiminto riittävän hyvä ja liiketoiminnan näkökulmasta järkevä. Tietoturvapäällikön mukaan *"nyt tiedetään asiakasvaatimuksia, mutta johdon pitää asettaa tavoite: liiketoiminnallisessa mielessä järkevä investointi taso"*. Tämän lisäksi haastateltujen mukaan haluttaisiin ymmärtää paremmin, mitä liiketoiminta-arvoa erilaiset ratkaisut palveluihin ja tuotteisiin liittyen tuottavat asiakkaalle.

Järjestelmien suorituskyky näkyy liiketoiminnalle usein palvelutasosopimusten kautta. Keskeinen tietotarve, joka haastatteluissa nousi esille, oli miten järjestelmät pystyvät vastaamaan palvelutasosopimuksiin. Johtotasolla ollaan kiinnostuneita siitä, miten myynnin neuvottelemat palvelutasot voidaan toteuttaa järjestelmissä. Johtoryhmälle taas riittää tieto siitä, ollaanko riittävän hyviä, muttei kalliita järjestelmien ja yleisesti tietoturvallisuuden kannalta. Yksi johtoryhmän jäsen totesikin tavoitteeksi, että kohdeyritys olisi *"maailman johtava ilman että sä oot maailman kallein*". Erään johtoryhmän ja yhden johtajan mukaan oikean rajanvedon löytäminen tietoturvallisuuden ja kustannusten välillä on tärkeää.

Mielenkiintoinen tietotarve tuli esille erään johtajan haastattelussa, jossa päädyttiin keskustelemaan tietoturvaan liittyvistä vastuista. Kaksi viikkoa ennen haastatteluja kohdeyrityksessä oli uudistettu tietoturvavastuita siten, että tuotteisiin liittyviä tietoturvavastuita on siirretty tuotepäälliköille. Tämä tarkoittaa käytännössä sitä, että tietoturvasta kohtalaisen tietämättömät henkilöt tekevät päätöksiä, joissa olennainen osa on tietoturvallisuus. Sisäiset tietoturvamittareiden liittäminen liiketoimintaan halutaan siis muodostaa siten, että niiden avulla tietoturvallisuudesta voidaan kommunikoida

Johtoryhmän tavoitteet tietoturvallisuudelle tuli esille asiakkaiden ja kokonaisuuden hallinnan kautta. Yhden johtoryhmän jäsenen mukaan tavoitteena on ansaita asiakkaiden luottamus täyttämällä heiltä saadut kriteerit, jotka pitää tulkita kohdeyritykselle olennaisin osin ja viedä ne eteenpäin alihankintaketjuun. Kaksi johtoryhmän jäsentä taas näki tietoturvallisuuden läpi arvoketjun, jonka tietoturvallisuuden pitäisi olla vakuuttavalla tasolla ja kuvattuna. Tavoitteena myös olisi, että käytännössä toimittaisiin kuvattujen prosessien mukaisesti. Yhden johtajan mukaan tietoriskit tulisi nostaa paremmin esiin kuin tällä hetkellä ja parantaa niiden näkemystä tietoturvallisuudesta, joilla siitä on

vastuu. Kaksi johtajaa taas näki, että kohdeyrityksen tulisi olla vaatimustenmukainen mahdollisimman kustannustehokkaasti. Toinen heistä täydensi, että tuotekehityksen kautta olisi tavoitteena pystyä automaattisesti täyttämään asiakasvaatimukset tärkeimmissä tuotteissa ja järjestelmissä.

6.2 Mitä mittauksen kohteita tunnistettiin?

Tulosten esittely ”mitä”-teeman suhteen jaetaan samoihin yläluokkiin, kuin ”miksi”-teemassa. Tässä luvussa pyritään tuomaan esiin näkökulmia siitä, mitä eri osa-alueissa mitattaisiin ja kartoittamaan, miten nämä osa-alueet suhtautuvat toisiinsa. Tietotarpeita tuodaan esille liiketoimintajohdon ja tietoturva-ammattilaisten näkökulmasta. Esimerkiksi sisäisten asioiden mittaaminen tukee tietoturvapäällikön työtä, mutta se vaatii liiketoiminnan määritelmät siitä, mitä mitattaisiin. Toisaalta asiakasnäkökulma vaikuttaa liiketoiminnan näkökulmaan mittauksen kohteista. Tuotekehityksen ja tietoturvallisuuden kehityksen avulla taas pyritään tuomaan parannuksia sisäiseen toimintaan, kuten riskien hallinta, ja vastaamaan paremmin asiakkaiden tarpeisiin.

6.2.1 Mittauksen kohteet osana sisäistä toimintaa

Lähtökohtaisesti tietoturvallisuuden mittaamisen ensimmäinen kohde tulisi olla se, ovatko kriittisimmät järjestelmät ja tiedot tunnistettu liiketoiminnan näkökulmasta ja liiketoiminnan muodostamin kriteerein. Tietoturvapäällikkö kertoi haastattelussa, että usein järjestelmät tunnistetaan tietotekniikan näkökulmasta, mutta tietoturvallisuuden liittäminen liiketoimintakontekstiin tulisi lähteä siitä, että liiketoiminta tunnistaa *”mitkä ovat kruunujalokivet”*. Tämän jälkeen voidaan ryhtyä löytämään tietotarpeille mittareita ja mittaamaan, miten hyvin tärkeimmät järjestelmät toimivat. Johdon näkökulmasta indikoitaisiin tieto siitä, miten hyvin tärkeimmät prosessit toimivat tietoturvallisuuden näkökulmasta.

Sisäisestä näkökulmasta järjestelmien ongelmat ja prosessin puutokset voidaan havaita mittareiden avulla. Tästä haastateltavat olivat liki yksimielisiä, mutta näkökulmat siitä, mistä ongelmia mitattaisiin, vaihtelivat. Johtoryhmätasolla oltiin yleisesti kiinnostuneita siitä, mitä sisäisesti tapahtuu. Esimerkiksi onko sisäisissä prosesseissa huomioitu tietoturvallisuus riittävän kattavasti ja toimivatko konkreettiset tietoturvatoiminnot prosessien mukaisesti. Käytännön toteutuksesta ei oltu kiinnostuneita. Yksi johtoryhmän jäsen pohti, voisiko sisäisen toiminnan mittaamisen ohella mitata ongelmien lisäksi myös positiivisia asioita. *"Me raportoidaan jokainen incidentti, mutta me ei raportoida sitä positiivista, joka päiväistä hyvää. Asiakas voisi olla tyytyväisempi jos me sitä pystyttäisiin mittaamaan”*. Eräs johtaja toi ongelmien kannalta hyvin käytännönläheisen näkemyksen. Hänen mukaansa kohdeyrityksessä saattaa olla ylläpitäjiä, jotka tietävät tarkasti missä järjestelmissä on ongelmia, mutta niitä ei tuoda esiin. Tämä johtuu esimerkiksi siitä, että ongelmat saatetaan kokea häpeällisinä.

Johtajat, joilla oli enemmän liiketoiminnallisia vastuita ja palvelutasosopimuksia, näkivät ongelmien mittaamisen asiakkaalle näkyvien tietoturvatapahtumien kautta. Palvelukatkot ja niihin johtaneet syyt nähtiin mittauksen kohteena. Tietoturva-asiantuntijoiden käsitys ongelmien mittaamisesta oli hiukan lähempänä käytännön toimintaa. Tietoturvapäällikkö oli kiinnostunut siitä, kuinka hyvin tietoturvatapahtumien havainnointi ja niihin reagointi saadaan liitettyä osaksi prosessia. Osana järjestelmien valvomista pitäisi siis osata tunnistaa tietoturvapoikkeamia tehokkaammin. Ylemmän johdon tietotarpeet olivat siis binäärisiä: onko tietoturvallisuus kunnossa vai ei? Tietoturva-asiantuntijoilla taas oli huomattavia vaikeuksia määritellä, milloin tietoturvallisuus on kunnossa ja milloin ei. Sisäisen mittaamisen teemaan olisi hyvä löytää mittari kuvailemaan tietoturva-asiantuntijoiden näkemystä, joka voidaan edelleen ilmaista johdolle heille suunnattujen mittareiden avulla.

Käytännön asia, jota sisäisessä toiminnassa pystytään mittaamaan, on tietoturvaprossien noudattaminen. Johtoryhmän mukaan nämä asiat tulee liittää riskeihin, laatuun, saatavuuteen ja tavoitettavuuteen. Näistä riskit ovat ainoa sisäisen toiminnan kannalta tärkeä asia, sillä muut mittauksen kohteet liittyvät siihen, miten asiakkaat näkevät kohdeyrityksen toiminnan ja jotka sisäisellä toiminnalla tulee varmistaa. Tietoturva-asiantuntijat toivat tähän liittyen esille käyttäjänhallinnan, jolla varmistetaan että vain valtuutetut henkilöt voivat käyttää tietoresursseja. Tietoturvatapahtumien havaitseminen oli tietoturvapäällikön näkökulmasta tärkeä mittauksen kohde, sillä sen avulla voidaan päätellä kykyä tunnistaa tietoturvaongelmia. Saatavuuteen ja tavoitettavuuteen taas pystytään tietoturvapäällikön ja kahden johtajan mukaan vaikuttamaan kapasiteetinhallinnan ja prosessinmukaisen päivittämisen avulla, jotka ovat hyviä mittauskohteita. Myös eräs johtoryhmän jäsen tiedosti väärään aikaan toteutettavien järjestelmäpäivitysten vaikeuttavan liiketoimintaa. Päivittäminen ja tietoturvaongelmat sekä niiden havaitseminen ovat yksi mittaamisen kohde.

Koulutusta ja sen tuomaa osaamista ei suoranaisesti nähty mittauskohteena, vaan pikemminkin sitä, onko olemassa oleva tietämys riittävä. Tämän mittaaminen ei ollut kaikista suurimpana tarpeena, mutta jollakin tapaa kohdeyrityksen henkilöstön tietämystä haluttiin varmistaa ja tietoisuutta nostaa asiakasvaatimusten tiukentuessa. Johtotasolla oli tosin luottamusta siihen, että henkilöstön tietämys on riittävällä tasolla. Yksi johtaja pohti henkilöstön osaamista prosessien noudattamisen kautta ja tiedosti, että niiden noudattamisessa on eroja tiimien välillä. Myös johtoryhmätasolla pohdittiin, miten hyvin sisäisiä prosesseja noudatetaan, onko niiden osalta kaikki kunnossa ja miten konkreettiset tietoturvakäytännöt toteutuvat niiden ohessa. Osaamisen mittaamista ei siis nähty kovinkaan tärkeänä, mutta kohdeorganisaation tietoturvakäytäntöjen noudattaminen oli sen sijaan selkeämpi mittauksen kohde.

6.2.2 Tietoturvallisuuden menestystekijät asiakasnäkökulmasta

Asiakasvaatimukset, joiden mukaan tuotteita kehitetään, ovat pääteema usealla liiketoimintalinjalla. Ymmärrys siitä, miten nämä vaatimukset vaikuttavat tietoturvallisuuteen, on jossain määrin huono. Vielä huonommin varsinkin johtoryhmätasolla ymmärretään, miten hyvin ja kattavasti asiakasvaatimukset jalkautetaan osaksi käytännön toimintaa. Tietoturvapäällikön näkökulmasta taas johtoryhmä ei aseta riittävän selkeitä vaatimuksia sille, miten hyvin asiakasvaatimuksia tulisi huomioida. Ongelman muodostaa muun muassa se, että eri asiakkailta saadut vaatimukset eivät ole yhdenmukaisia, vaan niiden painopisteet vaihtelevat huomattavasti. Sisäiseen näkökulmaan asiakasvaatimukset vaikuttavat usein siten, että niiden perusteella saatetaan joutua tekemään muutoksia tietoturvaratkaisujen suhteen. Nämä muutokset tuovat kustannuksia ja vaikeuttavat toimintaa. Kohdeyrityksen näkökulmasta olisikin tärkeää osoittaa oman toimintatavan hyöty asiakkaille ja näin välttyä asiakasvaatimusten aiheuttamilta muutoksilta. Asiantuntijan mukaan keino tähän on tehdä työ, prosessit ja tuotekehitys siten, että niistä jää todisteet toteutustavasta. Toteutustapa esitellään tarvittaessa asiakkaalle ja pyritään näin osoittamaan heille tärkeitä tietoturvatoimintoja.

Asiakkaan asettamat tavoitteet sisältävät kriteerejä, jotka tulee täyttää. Näiden kriteerien oikeanlainen priorisoiminen on johtoryhmän jäsenen mukaan tärkeää. Niiden kautta tulee pyrkiä ymmärtämään, miten asiakas näkee kohdeyrityksen tietoturvallisuuden. Tehokkaampi keino, asiakaspalaute, tuli esille useassa haastattelussa. Lisäksi kohdeyritys toteuttaa on asiakkaiden kanssa yhdessä auditoituja prosesseja. Näiden prosessien kautta voidaan ymmärtää, mikä on tärkeää asiakkaalle. Johtoryhmän jäsenen ja johtajan näkökulmasta olisi tärkeä tunnistaa, kuinka paljon asiakasvaatimusten tekeminen maksaa ja onko niiden kannalta menty eteenpäin sisäisessä toiminnassa siten, että oltaisiin jatkuvasti vaatimustenmukaisia. Tähän liittyy myös tuotekehitys, jonka avulla voidaan muiden haastateltavien paitsi johtoryhmän näkökulmasta vaikuttaa asiakasnäkökulmaan. Erään johtajan näkökulmasta asiakasnäkökulmaa on mahdollista tarkkailla sopimuksiin liittyvien kohtien kautta. Tällä hetkellä on tiedossa se, kuinka suuren riskin eri sopimukset kohdeyritykselle muodostavat. Tietoturvapäällikkö taas huomioi, että kaikkia asiakasvaatimuksia ei voida mitata.

Asiakasnäkökulmasta tärkeää on onnistua kaikissa tilanteissa, joissa asiakas kohdataan. Eräs johtoryhmän jäsen kuvaili tätä koko asiakasketjun läpäiseväksi ketjuksi ja huomioi siihen kuuluvaksi kaikki tapaukset aina asiakkaan tietoisuuden herättämisestä myyntilanteen kautta asiakkuuden hallintaan. Tähän ketjuun kuuluu niin imago, joka potentiaalisille asiakkaille on muodostunut ja myyntitilanne, johon kuuluu edellä esitellyt asiakasvaatimukset. Tämän jälkeen asiakkuudenhallintaan kuuluu asiakaspalvelu, jonka on annettava asiakkaalle tietoturvallinen vaikutelma. Myös muut johtoryhmän jäsenet toivat esille, että laadukkuus sisäisessä toiminnassa on tärkeää. Johtajille asiakasnäkökulma ja laadukkuuden osoittaminen näkyy palvelutasosopimusten kautta, joiden asettami-

en vaatimusten mittaaminen olisi tärkeää. Tietoturva-asiantuntijoiden näkökulmasta tämä asia nousi pinnalle sisäisten asioiden, kuten ongelmanratkaisun ja kapasiteetin hallinnan kautta, jotka vaikuttavat asiakasnäkökulmaan. Yksi mittauksen kohde voisi olla tunnistaa ne asiakaskohtaamispisteet, joissa tietoturvallisuudella on merkitystä ja varmistua, onko tietoturvallisuus huomioitu riittävällä tasolla niitä tukevassa sisäisessä toiminnassa.

Asiakasnäkökulmasta on tärkeää viedä vaatimuksia eteenpäin alihankkijoille ja osoittaa, että tietoturvallisuus on huomioitu myös tästä näkökulmasta arvoketjun läpi. Kaikki johtoryhmän jäsenet ja yksi johtaja tunnistivat tarpeen huomioida, miten toimittajille ja alihankkijoille viedään asiakasvaatimukset ja niihin liittyvät velvoitteet. Tällä hetkellä heidät velvoitetaan noudattamaan tiettyjä asioita sopimusteitse, mutta esimerkiksi aukkoja alihankintajärjestelmissä ei tunnisteta ja niiden oikeanlaista toimintaa ei pystytä todentamaan. Kaksi johtoryhmän jäsentä ja tietoturvapäällikkö pohtivat sitä, miten eri tahot pääsevät käyttämään kohdeyrityksen järjestelmiä ja mitkä jäljet niistä jää. Yksi johtaja taas pohti, että olisi tärkeää saada lisää läpinäkyvyyttä ja kokonaisuuden hahmottamista sille, mitä asioita on sovittu kumppanien kanssa. Toimittajille ja alihankkijoille muodostetut mittarit sopisivat osaksi koko arvoketjua kuvaavaa tietoturvamittaristoa, joka pitäisi yhden johtoryhmän jäsenen mukaan kuvata kunnollisesti ja kahden muun mukaan löytää niiden heikkoudet.

6.2.3 Tietoturvallisuuden ennakointi tuotekehityksessä

Erään johtoryhmän jäsenen mukaan tietoturvallisuus on osana päätöksiä siitä, minkälaisia tuotteita tehdään. Esimerkiksi omien myytävien tuotteiden tietoturvataso on tärkeä ymmärtää. Tähän liittyen uusien tuotteiden tietoturvauhkien esto nähdään tärkeänä. Yksi johtoryhmän jäsen pohti mahdollisuutta muodostaa joukko kriteerejä, joiden mukaan uuden tuotteen toimitusprosessi etenisi. Näiden kriteerien ohessa huomioitaisiin uusiin tuotteisiin liittyvät uhat ja tietoturvallisuuteen liittyvät asiat. Yhden johtajan mukaan tähän liittyen jokaiselle tuotteelle tulisi olla olemassa tietoturvasuunnitelma tuotannon ohessa. Lähes kaikki haastateltavat liittivät nämä asiat suoraan tuotekehitykseen, eli siihen että tietoturva-asiat huomioitaisiin jo osana tuotekehitystä. Esimerkiksi asiakasvaatimusten kautta voidaan muodostaa vaatimuslista, jonka avulla seurattaisiin tietoturvallisuuteen liittyvien ominaisuuksien kehitystä. Toinen keino on seurata suoriudutaanko asiakasvaatimuksista suoraan tuotekehityksessä vai ei. Tietoturvapäällikkö kuvaili tämän siten, että tuotteiden kehityksessä ja niiden tuotantoon saamisessa olisi suoraan tärkeää, ettei kehitetä tietoturvallisuuden kannalta huonoja tuotteita.

Tuotekehitykseen liittyen tietoturvallisuus nähtiin johtoryhmätasolla liittyvän laatuun ja sen kehitykseen, tarkkailuun ja sen aiheuttamien kustannusten arviointiin. Asiantuntija taas liitti tuotekehityksen laadun kehittämisen testaamiseen ja näki, että tutkivan kehitystyön lisääminen ja siihen panostaminen olisi hyvä keino parantaa laatua tietoturvallisuuden näkökulmasta. Laadun ohessa mittaamisen voi liittää siihen, miten hyvin asia-

kasvaatimuksista suoriudutaan ja miten sen suhteen on menty eteenpäin, kuten eräs johtaja asian kuvaili. Johtoryhmän jäsen taas näki, että kustannusten seuraaminen niiden asioiden suhteen, mitkä on jouduttu tekemään jälkikäteen, tarjoaa tilannekuvan siitä, mikä tietoturvallisuuden taso tuotekehityksessä on. Toisin sanoen paljonko maksaa tehdä jälkeenpäin asioita, joita ei tuotekehityksessä huomioitu.

Asiantuntija ja yksi johtaja mainitsivat, että yksi ongelma kohta on osittain suunnitellut tietoturvallisuuteen liittyvät projektit tai kehitystyöt, joita ei ole pystytty eri syistä toteuttamaan. Yhden johtajan ja asiantuntijan mukaan näiden asioiden suoriutumista voidaan mitata ja arvioida, miten ne kehittyvät ja ovatko ne viety käytäntöön. Tietoturvapäällikkö taas viitannee tähän joukolla prosesseja, joiden tietoturvallisuus ei ole kunnossa. Tämän ongelman ympärillä keskusteltiin myös johdon kanssa. Johdon edustajat tiedostivat, että tietoturvallisuuden resurssit eivät ole välttämättä riittävät. Näiden projektien ja kehittämistöiden priorisoiminen ja liiketoiminta vaikutusten arviointi voisi tukea ymmärrystä siitä, miten järjestelmät ja kohdeyrityksen toiminta pystyy vastaamaan muutokseen liiketoiminnassa.

6.2.4 Liiketoimintaan liitettävät mittarit

Tarve tietoturvallisuuden liittämisestä osaksi liiketoimintaprosesseja tunnistettiin niin johtoryhmässä, johdossa kuin tietoturva-asiantuntijoiden keskuudessa. Tietoturvapäällikön mukaan on tärkeää *"laittaa juuri tarpeellinen määrä resursseja eikä yhtään liikaa"*. Tietoturvakustannusten mittaaminen nähtiin kuitenkin todella haastavana. Esimerkiksi tietoturvallisuuteen kulutettua aikaa, joka on helppo muuttaa rahaksi, ei voida mitata kahdesta syystä. Ensinnäkin kohdeyrityksessä ei kohdisteta työaikoja ja toisekseen useassa tapauksessa on haastavaa määritellä, mikä on tietoturvallisuuteen liittyvää työtä ja mikä ei. Tietoturvallisuuteen kohdistettuja resursseja on haastattelujen perusteella hyvin haastava mitata myös siksi, ettei sitä ole eriytetty budjetissa. Eräs johtoryhmän jäsen kommentoi tietoturvakuluihin liittyen, että *"emmä tiedä miks mä sitä seuraisin"*. Häntä kiinnostaa miten tuotekehitysrahaa käytetään suhteessa siihen, mitä asiakas haluaa. Tämän avulla voisi ymmärtää esimerkiksi ongelmia ja käytettävyyteen liittyviä tekijöitä.

Yksi keino liittää tietoturvallisuus osaksi muuta toimintaa on toimia yleisesti tunnettujen toimialan parhaiden käytäntöjen mukaisesti. Eräässä toimialan sisäisessä vertailussa kohdeyritys onkin jo mukana tuotekehitysnäkökulmasta. Johtajan mukaan *"käytännössä tavotehan on se, että me oltais niinku "industry standard" -tyyppisesti complienttejä, eli tehdään ne asiat mitä muutkin tekevät niiltä osin kun ne on järkeviä"*. Myös johtoryhmän jäsen pohti, että olisi tärkeää tunnistaa miltä kohdeyrityksen tietoturvallisuus näyttää kilpailijoihin verrattuna. Nämä näkemykset tarkoittavat sekä sisäistä toimintaa, että asiakasnäkökulmaa. Sisäisen toiminnan kannalta resursseja ei siis pidä käyttää selkeästi enemmän kuin toimialalla yleisesti ja tuotteiden pitää olla asiakkaannäkökulmasta riittävän tietoturvallisia. Johtoryhmän jäsenen mukaan tavoitteena näihin voidaan pitää, että *"asiakasnäkökulmasta me ollaan niinku tietoturvallisuusmielessä maailman johta-*

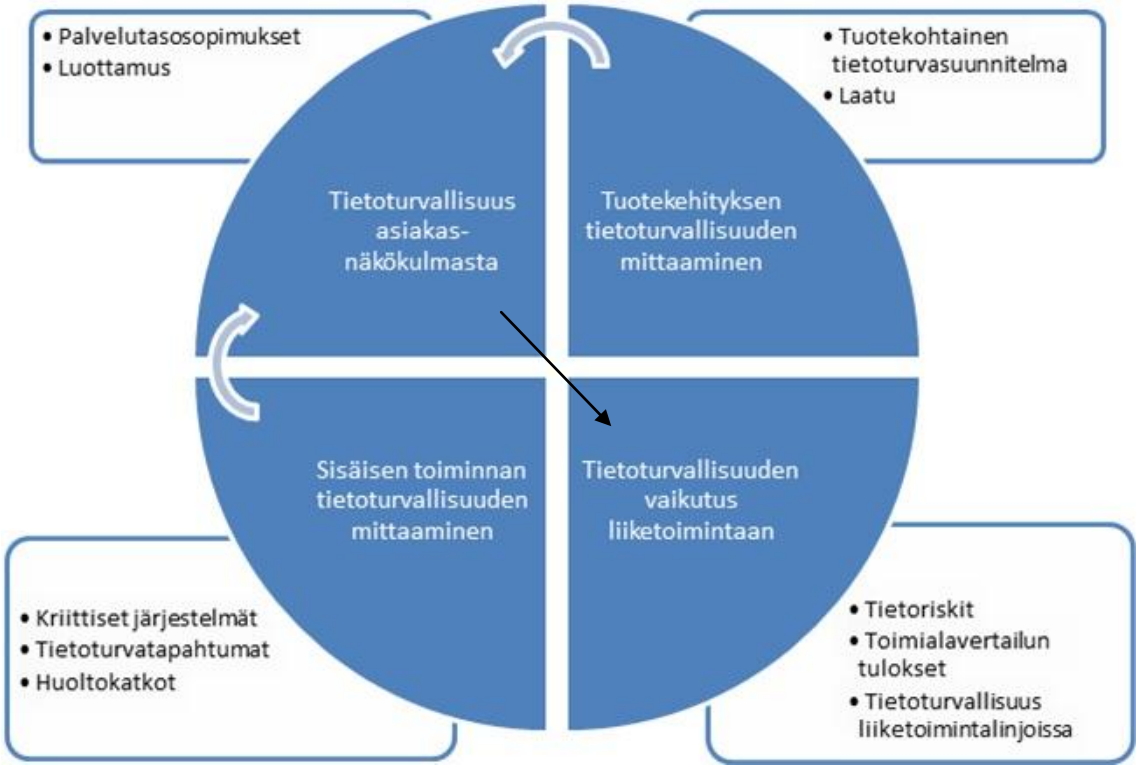
via, me tehdään oikeita asioita, me ei jäädä kiinni mistään typeryyksistä tai että meiän järjestelmät ei ollu tarpeeks hyviä”.

Tietoturvapäällikön mukaan johtoa kiinnostavat pahimmat tietoriskit ja se, mitä niille ollaan tekemässä. Johtoryhmän jäsenen mukaan on tärkeä seurata, mitkä ovat uhkakuvia ja mitä muualla on tapahtunut. Tähän hän kommentoi, että *”Riskinhallinta mielessä [tavoitteena on], et ei me yrityksen maine*”. Kohdeyrityksen maine nousi jossain määrin esille haastatteluissa, joista kahdessa pohdittiin maineen menetystä julkisuuteen tulleiden tietovuotojen kautta. Kohdeyritykselle on tärkeää, että tällaisia ei tapahdu heidän kohdallaan. Mittaamisen näkökulmasta todettiin, että näitä on kuitenkin hyvin haastava mitata. Maineeseen liittyvän riskin ohella johtoryhmän jäsenet mainitsivat sosiaaliseen mediaan ja sen käyttöön liittyvät riskit. Myös tietoturvapäällikkö esitteli yhden sosiaaliseen mediaan liittyvän relevantin riskin. Näitä kohdeyritys pyrkii hallitsemaan ohjeistuksella sosiaalisen median käytöstä. Toinen yksityiskohtainen riski, joka nousi johtoryhmässä esille, oli työntekijöiden omien laitteiden käyttö työn tekemiseen. Yleisesti oltiin kiinnostuneita siitä, mitkä ovat riskit liittyen tietoturvallisuuteen, mikä on niiden liiketoimintavaikutus ja miten niitä voidaan mitata.

Selkeä liiketoimintaan liitettävä mittauksenkohde tuli esille palvelutasosopimusten kautta. Yksi johtaja pohti, että palvelutasosopimukset eivät välttämättä aina ole viety järjestelmätasolle. Jos palvelutasosopimuksessa ei huomioida, että jokin palvelua tuottava järjestelmä ei ole riittävällä tasolla, aiheuttaa se ongelmia tiedon saatavuuteen ja tätä kautta kustannuksia sopimusrikkomuksesta johtuen. Toisaalta jos palvelutasosopimusten perusteella joudutaan tekemään muutoksia järjestelmiin, muodostuu ylimääräisiä kustannuksia. Mittauksen kohde voisi siis olla vertailu palvelutasosopimusten, joka on liiketoimintalähtöinen sopimus, ja järjestelmän ylläpitäjän vertailu siitä, voiko kyseisin palvelutason toteuttaa järjestelmällä. Tämän mittauksen yhteydessä on yhden johtajan mukaan mahdollista perustella laajemminkin erilaisten tietoturvallisuuteen liittyvien ratkaisujen arvoa asiakkaalle esimerkiksi sen kautta, kuinka moni asiakas tiettyjä ominaisuuksia vaatii. Toinen näkökulma on mitata, kuinka paljon maksaa poikkeuksellisten asiakasvaatimusten asentaminen järjestelmiin, eli mitkä ovat jälkikäteen tehtyjen räätälöintien kustannukset. Tämä mittari pitäisi johdon mukaan liittää myyjien työhön, sillä tällä hetkellä myyjät saavat bonuksensa huolimatta siitä, mitkä tehdyn kaupan lopulliset kustannukset kohdeyritykselle ovat.

6.3 Viitekehys tietoturvamittaristolle

Tulosten esittely ”miten”-teeman suhteen jaetaan samoihin yläluokkiin, kuin muiden teemojen esittely. Tässä luvussa esitellään toimintatutkimuksen toimintavaiheen lopputulos: tietoturvamittaristo. Lisäksi kuvaillaan, mihin tarkoitukseen mittaria käytetään ja minkälainen mittaus siihen liittyy. Kuvassa 6.1 esitellään mittariston viitekehys yleisellä tasolla, sekä se miten sen eri yläluokat liittyvät toisiinsa.



Kuva 6.1. Viitekehys tietoturvamittaristolle.

Viitekehys on rakennettu luvussa 3.3 esitellyn tasapainotetun tuloskortin mukaisesti, mutta sitä on muokattu kohdeyrityksen tarpeisiin sopivaksi. Jokaisen yläluokan oheen on suunniteltu muutama mittari, joiden avulla yläluokkaa pyritään kuvailemaan. Kokonaisuudessaan neljä yläluokkaa pyrkii esittämään, mikä tietoturvallisuuden tila on kohdeyrityksessä. Tilaa ei esitetä ”hyvänä” tai ”huonona”, vaan eri yläluokkien suoriutumista tulee verrata niille asetettuihin tavoitteisiin. Tavoitteiden asettaminen yläluokkiin liittyen onkin yksi suositus kohdeyritykselle. Lopullisena tavoitteena viitekehyksessä on tuoda tietoturvallisuus osaksi liiketoimintaa hahmottamalla, mitä kautta tietoturvallisuus näkyy liiketoiminnalle ja toisaalta miten liiketoiminta voi tukea tietoturvallisuutta.

Tasapainotetusta tuloskortista tuttu osaamisen näkökulma on vaihdettu tuotekehityksen näkökulmaksi. Toisaalta tuotekehityksen näkökulman ohessa huomioidaan osaaminen. Myös ongelmien mittaaminen ja niiden havaitseminen tukee tietoturvatietoisuuden lisääntymistä. Viitekehyksessä olennaisena asiana kohdeyrityksen toiminnan kannalta on asiakasnäkökulma, joka vaikuttaa yrityksen liiketoimintaan. Johtoryhmän jäsenten mukaan tietoturvallisuus halutaan nähdä asiakkaan kautta. Kuvassa 6.1 esitetyt vaaleansiniset nuolet kuvastava sitä, miten tietoturvallisuus näkyy asiakkaalle. Kun tietoturvallisuus näkyy asiakkaalle sisäisen toiminnan ongelmien kautta, vaikuttaa se liiketoimintaan esimerkiksi sopimusrikkomusten tai pahimmillaan menetettyjen asiakkaiden muodossa. Tuotekehityksen kautta kohdeyritys pystyy lisäämään asiakkaiden luottamusta ja osoittamaan, että se kehittää tietoturvallisia tuotteita ja palveluita. Musta viiva kuvastaa sitä, että asiakkaiden päätöksillä on suora vaikutus liiketoimintaan. Seuraavaksi esitel-

lään viitekehykseen liittyvät mittarit, joiden avulla kohdeyrityksen tietoturvallisuuden tilaa pyritään hahmottamaan kokonaisuutena.

6.3.1 Sisäisen toiminnan tietoturvallisuuden mittaaminen

Kriittiset järjestelmät

Perustelu
Haastatteluissa tuli ilmi, että kohdeyrityksessä ei ole tunnistettu liiketoimintakriittisiä järjestelmiä liiketoiminnan edustajien näkökulmasta. Brotbyn (2009, s.297) mukaan liiketoiminnan mahdollistaminen ja sen tavoitteiden tukeminen on järjestelmäarkkitehtuurin pääasiallinen tavoite. Näiden järjestelmien tunnistaminen tukee tietoturvapäällikön työtä ja auttaa liiketoiminnan edustajia kuvaamaan tietoturvallisuutta kokonaisuudessaan liiketoimintalinjoissa.

Kuvaus
Esimerkiksi jatkuvuussuunnitteluprojektin ohessa olisi mahdollista tehdä analyysi siitä, kuinka suuri osa järjestelmistä on tunnistettu siten, että niiden vaikutus liiketoimintaprosesseihin ymmärretään. Jatkuvuussuunnitelman perusteella järjestelmille pystytään jatkossa antamaan suorituskykyyn liittyviä vaatimuksia, arvioimaan niiden riskejä ja suunnittelemaan miten mahdollisista virheistä voidaan toipua. Mittaus vaatii listauksen yrityksen kaikista järjestelmistä, jotta prosenttiosuus analysoiduista järjestelmistä voidaan laskea.

Mittaus
Prosenttiosuus niistä järjestelmistä, joihin on tehty kuvauksenmukainen analyysi. Seurataan trendiä.

Tietoturvatapahtumat

Perustelu
Tietoturvatapahtumista aiheutuvat ongelmat ja häiriöt saattavat näkyä asiakkaalle ja vaikuttavat sitä kautta liiketoimintaan. Tietoturvallisuudessa havaittuja tai siihen liittyviä ongelmia poistamalla ja vähentämällä voidaan parantaa laatua, joka näkyy asiakkaille esimerkiksi palveluiden saatavuuden kautta. Tietoturvatapahtumia seuraamalla voidaan havaita heikkoja lenkkejä toiminnasta.

Kuvaus
Tietoturvatapahtumiksi voidaan tämän mittarin kohdalla laskea kaikki tietoturvallisuuteen liittyvät ongelmat, jotka vaikuttavat liiketoimintaan tai joiden oletetaan vaikuttavan liiketoimintaan. Esimerkiksi prosessien puutokset ja kriittiset tietoturvatapahtumat ovat liiketoimintaan liittyviä ongelmia. Eräs johtaja kuvaili ongelmia seuraavasti: *”Ongelmat tulee esiin, jos niitä kysytään. Kysymyspatterin pitäisi olla strukturoitu/jäsennelty, jossa*

käytäisiin läpi yhteiset pelisäännöt, ja saataisiin vastauksia siitä, missä ongelmakohtia on kootusti ja koordinoidulla tavalla". Ongelmien ja häiriöiden havaitsemista voidaan tehostaa myös yleisellä tasolla tämän ajatuksen perusteella. Tietoturvatapahtumat voidaan priorisoida karkeasti sen mukaan, mihin järjestelmään ne vaikuttavat. Omien prosessien riskitasojen mukaan tehdään päätökset siitä, miten tapahtumiin reagoidaan. Toisaalta tietoturvatapahtumia seuraamalla voidaan havaita uusia tietoriskejä.

Mittaus
Seurataan tietoturvaan liittyvien ongelmien ja häiriöiden määrää eri järjestelmissä vakavuuden, keston ja ongelman aiheuttaman riskin mukaan. Kokonaisvaltaista kuvaa varten muodostetaan liiketoimintalinjakohtainen trendi tietoturvatapahtumien määrästä. Verrataan havaitsijan antamia korkean vakavuuden riskiarvioita johtajan arvioon.

Huoltokatkot

Perustelu
Esimerkiksi päivittäminen on välttämätön keino siihen, että järjestelmät pidetään ajan tasalla ja niiden tila tunnetaan jatkuvasti (Jaquith 2007, s. 59). Päivittäminen näkyy liiketoiminnalle käyttökatkoina, joiden aikana kriittiset järjestelmät eivät toimi ja siten tuota liiketoimintahyötyjä. Myös muut huoltokatkot, esimerkiksi palvelinten uudelleenkäynnistämiset, muodostavat käyttökatkoja. Joskus uudelleen käynnistäminen on pakko toteuttaa, jotta vältytään pidemmältä käyttökatkolta.

Kuvaus
Suunniteltujen huoltokatkojen ulkopuolella tehdyt päivitykset ja järjestelmien uudelleenkäynnistys näkyvät pahimmillaan asiakkaalle. Tästä syystä niitä ei tulisi tehdä. Kohdeyritys voi pyrkiä tähän mittaamalla huoltokatkojen aiheuttamien suunnittelemattomien käyttökatkojen määrää.

Mittaus
Mitataan huoltokatkojen ulkopuolella tehtyjen päivitysten tai järjestelmien uudelleen käynnistysten määrää järjestelmäkohtaisesti ja seurataan trendiä. Tietoa voidaan myös verrata huoltokatkojen aikana tehtyjen päivitysten määrään, jolloin trendi voidaan suhteuttaa kokonaisuuteen.

6.3.2 Tietoturvallisuus asiakasnäkökulmasta

Palvelutasosopimukset

Perustelu
Eräs johtoryhmän jäsen painotti, että sisäinen toiminta on tärkeää, mutta se pitää nähdä asiakkaan kautta. Palvelutasosopimukset ovat olennainen osa kohdeyrityksen liiketoi-

mintaa ja niihin liittyvät ongelmat aiheuttavat kustannuksia. Toisaalta palvelutasosopimukset aiheuttavat kustannuksia, mikäli niistä tehdään liian vaativia, jolloin joudutaan tekemään muutoksia palveluita tuottavissa järjestelmissä.

Kuvaus
Sisäisen toiminnan ongelmia mitatessa voidaan antaa suurempi riskiluokitus niiden järjestelmien ongelmille, jotka vaikuttavat palvelutasosopimusten alaisiin palveluihin. Liiketoiminnan näkökulmasta palvelutasosopimuksia, jotka liiketoiminnan edustaja muodostaa tulee tarkastella myös taustajärjestelmän ylläpitäjän kanssa. Näin voidaan ennakoiden arvioida, pystyykö kohdeorganisaatio toteuttamaan sovitun palvelutason.

Mittaus
Vertailu siitä, miten asiakkaan kanssa neuvotellun palvelutasosopimuksen vaatimukset pystytään toteuttamaan olemassa olevilla järjestelmillä. Järjestelmän ylläpitäjä arvioi sopimuksen toteutettavuuden asteikolla 1-5. Lisäksi seurataan sopimuksista aiheutuneiden muutosten keskikustannuksia. Vertaillaan toteutettavuuden trendiä keskikustannusten muutokseen.

Luottamus

Perustelu
Kohdeyrityksen toiminta näkyy asiakkaalle ongelmien ja sopimusten lisäksi asiakaskohtauspisteissä. Osassa näistä tietoturvallisuudella on suuri merkitys, esimerkiksi asiakasta tunnistettaessa tietoturvallisuus tulee huomioida. Liiketoiminnan kannalta olennaisempaa on, että kaikissa kohtaamisessa voidaan seurata asiakkaan luottamusta kohdeyritykseen.

Kuvaus
Liiketoiminnan näkökulmasta voidaan seurata, kuinka paljon asiakkaat luottavat kohdeyrityksen tietoturvallisuuteen ja kuinka turvalliseksi he tuotteet kokevat. Näitä asioita voidaan kysyä asiakkailta erilaisissa kohtauspisteissä ja hyödyntää tuloksia osana myyntiä.

Mittaus
Asteikolla 1-10, kuinka paljon asiakas luottaa kohdeyritykseen.
Asteikolla 1-10, kuinka tietoturvalliseksi asiakas kokee kohdeyrityksen tuotteet tai palvelut.

6.3.3 Tuotekehityksen tietoturvallisuuden mittaaminen

Tuotekohtainen tietoturvasuunnitelma

Perustelu

Usean haastatellun mukaan tuotekehityksen ja tuotteiden toimituksen oheen tulisi muodostaa kriteeristö, jossa käydään läpi uhat ja tietoturvaan liittyvät asiat. Landwehrin (2001) mukaan tuotteen toimintavarmuuden voi osoittaa kolmella tavalla. Nämä ovat työntekijöiden osaamisen todistaminen, käytettyjen prosessien laadun osoittaminen ja tuotteen testauksen osoittaminen.

Kuvaus
Tietoturvasuunnitelman tulisi sisältää kohdeyrityksen toimintaan sopien lista vaaditusta osaamisesta, prosessin laatutyökaluista ja laadun valvonnasta. Tuoteprosessin edetessä listan avulla seurataan, täyttääkö tuote sille asetetut vaatimukset ja kriteerit. Asiakasvaatimukset huomioidaan osana vaatimuksia. Lisäksi annetaan asiantuntijoille mahdollisuus vaikuttaa tarkastuslistan sisältöön ja huomioidaan siinä ajankohtaiset tietoriskit. Listoja tulee lisäksi ylläpitää, eli huomioida niissä ajan myötä muuttuvat vaatimukset. Vaatimuksia voidaan löytää esimerkiksi tietoriskejä tunnistamalla. Tietoturvasuunnitelmasta muodostaan tuotepäälliköiden työkalu, jonka avulla he voivat varmistaa että tuotteet läpikäyvät vaaditun prosessin ja täyttävät tietoturvavaatimukset.

Mittaus
Mitataan kunkin tuotteen kohdalla, kuinka suuren osan asetetuista vaatimuksista se täyttää. Mittauksista voidaan muodostaa kokonaisuus, jonka trendiä voidaan seurata.

Laatu

Perustelu
Johtoryhmä näkee tietoturvallisuuden laadun kautta. Tuotekehityksessä laatu tulee huomioida alusta asti sillä löydetyistä virheistä koituvat kustannukset kasvavat huomattavasti mitä myöhemmin ne löydetään (Brotby 2009, s. 16). Asiantuntija täsmensi, että tuotekehityksessä tulisi tehdä enemmän tutkivaa kehitystyötä, jossa kehitetään testausmenetelmiä. Kujansivu et al. (2007, s. 181) taas pitävät automatisoitujen prosessien osuutta yhtenä teknologian hyödyntämiseen liittyvänä mittariaihiona.

Kuvaus
Annetaan resursseja tutkivalle kehitystyölle ja pyritään lisäämään tuotteiden tietoturvatestauksen automaatiota.

Mittaus
Täysin automatisoitujen tietoturvatestien osuus kaikista tietoturvatesteistä.

6.3.4 Tietoturvallisuuden vaikutus liiketoimintaan

Tietoriskit

Perustelu

Johdon tietotarpeena tuli esille ymmärtää tietoturvallisuuteen liittyviä riskejä ja isoja kokonaisuuksia, jotka voivat vaikuttaa kohdeyrityksen toimintaan tai jotka voivat vaikuttaa asiakkaiden ja sidosryhmien näkemykseen kohdeyrityksen tietoturvallisuuden tasosta.

Kuvaus
Riskien näkökulmasta voidaan mitata kohdeorganisaation kykyä havaita riskejä. Esimerkiksi tuotekohtaisen tietoturvasuunnitelman ja järjestelmien tietoturvakartoituksen ohessa voitaisiin tunnistaa riskejä, jotka vaikuttavat liiketoimintaan. Ulkopuolelta tulevien riskien kohdalla voisi olla mahdollista luottaa henkilöstön osaamiseen ja kannustaa havaitsemaan uusia tietoriskejä esimerkiksi leikkimielisellä kilpailulla. Havainnoinnin lisäksi riskejä tulee arvioida formaalein riskienhallinnan keinoin ja tehdä päätöksiä siitä, miten niihin reagoidaan.

Mittaus
TOP 5 tietoriskit ja niihin liittyvät toimintaehdotukset liiketoimintalinjoittain.

Toimialavertailun tulokset

Perustelu
Johdon ja johtoryhmän edustajien mukaan kohdeyritykselle on tärkeää olla toimialan johtava tietoturvallisuuden näkökulmasta. Brotbyn (2009, s. 197-198) mukaan tietoturvallisuuden tulisi tukea organisaation mainetta siten, että se on kilpailukykyinen verrattuna toimialan yleiseen tasoon ja luo luottamusta sidosryhmille.

Kuvaus
Toimialavertailun tulos ja sitä heikentävät tekijät esitetään johdolle muiden tietoturvaraporttien yhteydessä.

Mittaus
Sijoitus toimialavertailussa. Trendi siitä, miten on kohdeyrityksen sijoitus on muuttunut ja perustelu muutokselle.

Tietoturvallisuus liiketoimintalinjoissa

Perustelu
Johtoryhmä kaipasi kokonaisvaltaista kuvaa tietoturvallisuudesta, jonka avulla voidaan hahmottaa mistä kohdeyrityksen tietoturvallisuudessa on kyse ja miten kohdeyritys suoriutuu vaatimuksistaan.

Kuvaus

Koko kohdeyrityksen tietoturvallisuus tulee nähdä liiketoimintalinjojen kautta. Liiketoimintalinjojen toiminnan kuvaamisen yhteydessä tulee tunnistaa teknologiat, prosessit ja ihmiset, jotka ovat kriittisimpiä tietoturvallisuudelle. Tämän jälkeen voidaan edellä esiteltyjä mittareita kohdistaa niihin toimintoihin jotka nähdään tärkeinä. Apukysymyksinä voidaan käyttää esimerkiksi seuraavia: ”Mitkä ovat liiketoimintalinjan kriittiset järjestelmät, mitä ongelmia niissä ilmenee ja päivitetäänkö niitä prosessin mukaisesti?”, ”Miten liiketoimintalinjan tuotteiden ja palveluiden tietoturvallisuus parantuu?” ”Miten liiketoimintalinja onnistuu asiakaskohtauspisteissä ja asiakkaiden näkökulmasta?” Korkeatasokuvauksen perusteella voidaan muodostaa tavoitteita ja yksityiskohtaisempia mittareita liiketoimintalinjojen tietoturvallisuudelle kriittisistä asioista ja viestiä liiketoimintalinjan johtajan asettamia tavoitteita tietoturvallisuudesta.

Mittaus
Kuinka hyvin liiketoimintalinjan tietoturvallisuus on kuvattu asteikolla 1-10.

6.4 Mittariston arviointi

Toimintatutkimuksen viimeiset vaiheet, eli toiminnan arviointi ja tutkimuksen löydösten arviointi toteutetaan tässä luvussa. Löydöksenä pidetään mittaristoa, jota suositellaan kohdeyritykselle. Luvun 6 rakenne perustuu täysin kuvassa 5.1 esiteltyyn mittaristoprojektiin, jonka lopputuloksena tietoturvamittaristo muodostettiin. On siis huomattava, että mittariston kehitysprojektia voidaan jo itsessään pitää löydöksenä ja suosituksena sille, miten kohdeyritys voi tunnistaa mittareita käyttöönsä. Kohdeyrityksen edustajien arvio perustuu avoimeen haastatteluun edustajien kanssa. Mittaristo esiteltiin kohdeyritykselle joulukuussa 2012, jonka perusteella siitä pyydettiin arvioita soveltuvuudesta käytäntöön. Kirjallisuus näkökulman kriteerit, taas on esitetty luvussa 3.4 tehdyillä löydöksillä. Näitä ovat muun muassa Lippmannin et al. (2012) muodostamat kriteerit siitä, että mittareiden tulee:

- olla helposti ymmärrettäviä ja riittävän käytännön läheisiä
- arvioida täsmällisesti jotain riskiä, jonka organisaatio on tunnistanut
- tukea käytäntöjä, joilla riskejä hallitaan.

Näiden tekijöiden lisäksi mittareita on arvioitu myös subjektiivisuuden ja objektiivisuuden näkökulmasta sekä niiden validiteetin ja reliabiliteetin perusteella. Esimerkiksi Kujansivu et al. (2007, s. 162, 169-170) suosittelevat, että mittareita arvioidaan näiden tekijöiden perusteella. Mittareita arvioidessa on hyvä tunnistaa, ovatko ne muodostettu subjektiivisesti vai objektiivisesti, jotta voidaan ymmärtää niiden reliabiliteettiin vaikuttavia tekijöitä. Jaottelu subjektiivisiin ja objektiivisiin mittareihin auttaa myös arvioimaan mittareiden muita ominaisuuksia, kuten mitä valmistelutoimenpiteitä mittaaminen vaatii ja mitä miten mittauksen kohde linkittyy johonkin menestystekijään.

6.4.1 Mittariston soveltuvuus kohdeyritykselle

Mittariston soveltuvuuden arviointia kohdeyrityksen näkökulmasta ei onnistuttu täysin suorittamaan. Avoimeen haastatteluun, joka toteutettiin sähköpostitse, osallistui vain kolme kahdeksasta teemahaastatteluun osallistuneesta. Suurin ongelma on, että yksikään johtoryhmän edustaja ei vastannut arviointipyyntöön. Tästä voidaan päätellä, että suunnitellun mittariston arviointiin ei haluttu käyttää aikaa, koska se ei vastannut kohdeyrityksen johdon odotuksia, eikä siten sovellu heidän käyttöönsä. Näin tarkasteltuna voidaan todeta, että mittaristo ei läpäissyt Jaquithin (2007, s. 25, 27) esittelemää ”So what?”-testiä ja vaatii näin ollen jatkokehitystä.

Toisaalta myös muita syitä vastaamattomuuteen voidaan löytää. Ensinnäkin suuri haaste toimintatutkimuksen suorittamiselle on, että ulkopuolisella tutkijalla ei ole täyttä kohdeyrityksen edustajien luottamusta (Levin et al. 2002). Tietoturvallisuus itsessään on aihepiiri, jossa luottamus on vaikea ansaista ja johon liittyvän tiedon jakamisessa ollaan erityisen tarkkoja. Lisäksi tietoturvallisuus ei ole korkeimman johdon tärkeimpien asioiden listalla ja diplomityö on tutkimus, jonka lopputulosten ei välttämättä odoteta olevan kattavia ja käytännönläheisiä. Näistä syistä vastaaminen arviointipyyntöön oli helppo jättää tekemättä. Tämän lisäksi tutkimusta ei tehty riittävän läheisessä yhteistyössä kohdeyrityksen johdon kanssa, vaan kommunikointi tapahtui tietoturvapäällikön kanssa. Näin ollen johto jäi etäiseksi teemahaastatteluja lukuun ottamatta eikä siten aktiivisesti ollut kiinnostunut tutkimuksen etenemisestä. Iversenin et al. (2004) mukaan toimintatutkimuksessa tärkeä menestystekijä onkin hyvä ja läheinen suhde tutkimuksen kohteen kanssa, mitä tämän tutkimuksen aikana ei saavutettu. Hyvä suhde ja läheinen kanssakäyminen johtoryhmän kanssa olisivat varmasti lisänneet avoimeen haastatteluun vastanneiden määrää.

Kohdeyrityksen tietoturvapäällikön näkökulmasta positiivista on, että mittaristo on tiivis, mikä lisää mahdollisuuksia sen käyttöönotolle. Tätä tukee myös se, että mittaristo heijastaa johtoryhmän tahtotilaa ja se on perusteltu huolellisesti. Asiantuntija arvioi, että yleisellä tasolla mittaristolle on tällä hetkellä tarve, mutta silti on kyseenalaista, kuinka vahvasti se tullaan viemään käytäntöön. Vaikka mittarit ovat kohdeyrityksen edustajien mukaan lähtökohtaisesti helposti ymmärrettäviä, vaativat tietyt mittarit, kuten tuotekohtainen tietoturvasuunnitelma ja tietoturvatapahtumat, liian laajoja toimenpiteitä. Kokonaisuudessaan mittaristo on johtajan mukaan hyvä vastaus kysymykseen ”Mistä kaikesta kohdeyrityksen tietoturvallisuuden pitäisi koostua?”.

Yksityiskohtaisemmalla tasolla johtaja arvioi, että tuotekohtaisen tietoturvasuunnitelman laajuuden ja monipuolisuuden sijaan olisi voinut suunnitella yksinkertaisemman mittarin. Mittari voisi kuvailla yksinkertaisesti sitä, pystytäänkö tärkeimpien asiakkaiden asettamia vaatimuksia täyttämään ja mikä on käytännön toiminnan ero vaatimuksiin nähden. On kuitenkin huomattava, että tämän kaltainen mittari on itsessään osa suunni-

teltua tuoteprosessin mittaamista. Tietoturvallisuuden kuvaaminen liiketoiminta linjoissa taas vaatisi edelleen työtä kuvausmenetelmän kehittämiseksi. Mittareiden kuvausten ja niiden visualisoinnin kehittäminen ovatkin relevantteja jatkotutkimuksen kohde yhdessä käyttöönoton suunnittelun kanssa. Suurin kokonaisuus, jota mittaristosta jäätiin kaipaamaan, oli tietoturvakustannukset. Näiden esiintuominen vaatisi tosin oman tutkimuksensa ja todella syvällisen ymmärryksen kohdeyrityksen tietoturvallisuudesta.

Suurin ongelma, joka mittareissa havaittiin, oli niiden tulosten ymmärrettävyys. Asiantuntijan mukaan tämä ongelma on kohdeyrityksen näkökulmasta yleinen mittaamisen ongelma, joka korostuu tietoturvallisuutta mitattaessa. Esimerkiksi suurimpien tietoriskien mittaaminen muuttuu helposti osaoptimoinniksi, jossa suurinta osaa riskeistä ei hallita riittävän kattavasti. Tuloksena on, että huonon arvion seurauksena suuri riski jää osaksi liiketoimintaa. Kaiken kaikkiaan suurin osa mittareista arvioitiin hyviksi ja avoin palaute muodostui käyttöönoton ongelmien pohtimisesta. Osa mittareista, kuten luottamus ja kriittiset järjestelmät, soveltuu erinomaisesti kohdeyrityksen käyttöön. Kohdeyrityksen suhtautuminen mittaamiseen on sekä yleisesti että suunnitellun mittariston kannalta kuitenkin haluton. Motivaatiota järjestelmälliselle mittaamiselle ei ole, kuten jo teemahaastatteluissakin kävi ilmi.

6.4.2 Mittariston arviointi kirjallisuuden näkökulmasta

Mittaristossa esitellään sekä objektiivisia että subjektiivisia mittareita. Objektiivisista mittareista laadun mittari on muodostettu siten, että se kertoo kuinka suuri osuus tietoturvatesteistä tehdään automatisoidusti. Mittari on hyvin epäsuora ja se kannustaa kehittämään testaustyöskentelyä laadun parantamiseksi. Päivittäminen on sen sijaan suoraan saatavuutta kuvaileva mittari, joka on helposti ymmärrettävä ja toteutettava. Objektiivisina mittareina voidaan pitää myös tunnistettujen kriittisten järjestelmien määrän mittaamista ja tuotekohtaista tietoturvasuunnitelmaa. Näillä mitataan kuinka hyvin kohdeyritys tuntee ympäristönsä tietoturvallisuuden näkökulmasta ja kuinka hyvin kohdeyrityksessä suoriudutaan asetetuista vaatimuksista. Suoraa kuvaa tietoturvallisuudesta objektiiviset mittarit eivät anna. Vaatimusten asettaminen objektiivisia mittareita varten on hyvin subjektiivista. Kriittisten järjestelmien ja tuotekohtaisten mittareiden muodostamiseksi joudutaan tekemään huomattava määrä päätöksiä esimerkiksi siitä, milloin vaatimus täytetään ja milloin ei. Lisäksi on asetettava tavoitteita sille, mitkä vaatimukset tulee täyttää eri tuotteiden osalta. Kriittisten järjestelmien osalta taas tehdä päätöksiä siitä, mitkä ovat kriteerit joiden perusteella järjestelmät tunnistetaan. Toisaalta näiden mittareiden huolellinen valmistelu ja kriteerien asettaminen auttaa esimerkiksi tietoturvatapahtumien mittaamisessa, joka on vahvasti subjektiivinen mittari.

Täysin subjektiivisia mittareita ovat toimialavertailu, tietoriskit ja palvelutaso. Tietoriskien mittarin objektiivisuutta voidaan lisätä käyttämällä formaalia riskienhallintaprosessia, jolloin riskien vertailu ja niiden arviointia tehdään mahdollisimman samalla tavalla ja samoin perustein. Voidaan myös nähdä, että mitä paremmin kohdeyritys tuntee sisäi-

sen toimintansa ja osaa mitata tietoturvatapahtumiaan sitä parempi reliabiliteetti sen riskiarvioinneissa on. Toimialavertailu ja palvelutaso taas tukevat toimintaympäristön tuntemista. Toimialavertailu kuvailee epäsuorasti, miten hyvä tietoturvallisuus kohdeyrityksellä on muihin samankaltaisiin yrityksiin verrattuna. Palvelutason mittaaminen auttaa kohdeyritystä ymmärtämään, miten hyvin sisäinen toiminta vastaa asiakkaiden tarpeisiin. Varsinkin sijoitus toimialavertailussa on helppo ottaa raportointiin mukaan ja liittää siihen trendi aikaisemmista sijoituksista. Myös tietoriskit on käytännöllistä nostaa mukaan raportointiin. Lisäksi niiden tunnistaminen motivoi arvioimaan ja hallitsemaan riskejä yleisemmällä tasolla. Palvelutason mittaaminen sen sijaan vaatii hiukan valmisteluja ja yhteistyön kehittämistä liiketoiminnan ja järjestelmäasiantuntijoiden kanssa, mutta on tämän jälkeen helposti ymmärrettävä ja käytännön läheinen mittari.

Asiakkaiden luottamus on tärkeä kilpailukykyä edistävä seikka, jota asiakaskohtauspisteissä voidaan arvioida. Luottamus on vahvasti subjektiivinen mittari, joka kuvailee asiakkaiden mielipiteitä. Lisäksi luottamus menetetään helposti, joten hyvätkään tulokset tästä mittarista eivät takaa sitä, että kohdeyrityksen tietoturvallisuus olisi huippuluokkaa. Objektiiviset mittarit, laatu ja päivittäminen, tukevat sitä, että luottamus säilytettäisiin. Tuotekohtainen tietoturvasuunnitelman tavoitteena taas on parantaa prosessinhallintaa, jonka avulla tietoturvallisuutta voidaan kehittää ja näin parantaa asiakkaiden luottamusta kohdeyritykseen. Luottamuksen reliabiliteettia voidaan lisätä keräämällä mittariin runsaasti vastauksia ja muodostamalla näistä trendi, joka kuvastaa muutosta ajan suhteen. Yleisesti kaikille mittareille on yhteistä, että yksittäinen mittaus ei kuvaile kohdeyrityksen tietoturvallisuuden tilaa kovinkaan hyvin. Mittaamisen prosessiin liittyy olennaisesti mittariston ylläpito, joissa arvioidaan käytöstä saatujen kokemusten perusteella mittareiden hyvyyttä ja päivitetään niitä tarpeenmukaisesti. Ylläpidollisten toimien ohessa tulee aina arvioida, vastaako mittari edelleen johonkin tavoitteeseen. Menetelmiä kehittämällä ja selkeitä tavoitteita asettamalla mittareiden reliabiliteettia ja validiteettia voidaan parantaa.

Mittariston kehittämiseen liittyy olennaisesti mittaamisen maturiteettitasot, jotka esiteltiin luvussa 4.5. Suurin osa esitellyistä mittareista on implementoinnin mittareita, jotka soveltuvat prosessien vakauttamiseen ja oman toiminnan tuntemisen kehittämiseen. Tietoturvatoimintojen kyvykkyyttä kuvailevat huoltokatkot ja tietoturvatapahtumien mittaaminen. Tietoturvallisuutta sidosryhmien näkökulmasta kuvailevat toimialavertailu ja luottamus. Jossain määrin myös riskeistä ja palvelutason mittaamisesta voidaan päätellä tietoturvallisuuden kykyä vastata liiketoiminnan tarpeisiin tai siihen liittyviin uhkiin. Mikään mittari ei pysty automaattisesti keräämään dataa, vaan ne tulee toteuttaa jonkun muun prosessin tai toiminnan yhteydessä. Tästä syystä mittarit voidaan ottaa käyttöön suhteellisen helposti. Esimerkiksi huoltokatkot, palvelutaso, toimialavertailu ja luottamus vaativat vain pienen muutoksen raportointiin tai toimintaan. Toisaalta esimerkiksi tuotekohtainen tietoturvasuunnitelma ja kriteerit kriittisten järjestelmien tunnistamiselle ovat raskaita toteuttaa, vaikka itse mittarit ovat yksinkertaisia.

Useat esitellyistä mittareista ovat samankaltaisia, kuin kirjallisuudesta löytyvät mittarit. Puhtaasti tietoturvallisuuden mittaamiseen liittyy vain huoltokatkojen mittaaminen, jonka Jaquith (2007, s. 60-61) esittelee. Muut mittarit ovat hyvin samankaltaisia muihin liiketoiminnan mittaamistilanteisiin verrattuna. Esimerkiksi palvelutason mittaamista toteutetaan aina varsinkin saatavuuden näkökulmasta. Tässä tutkimuksessa esitetty mittari tosin pyrkii tuomaan palvelutasosopimusten liiketoimintavaikutusten ymmärtämiseen syvyyttä. Tietoturvatapahtumien mittaaminen on perinteistä liiketoimintaan liittyvien häiriöiden hallintaa ja häiriöihin liittyvää mittaamista, johon on olemassa kypsiä tapoja esimerkiksi häiriöiden taajuuteen, häiriöistä toipumiseen ja niiltä suojautumiseen liittyen (mm. Jaquith 2007, Savola 2007, CIS 2009). Tietoturvatapahtumien avulla voidaan tunnistaa tietoriskejä, joiden mittaaminen on korkealla tasolla samankaltaista kuin muidenkin liiketoimintariskien mittaaminen.

Jokseenkin yllättävää on, että mittaria asiakkaiden luottamukseen liittyen ei kirjallisuudesta löydetty. Tämä mittari soveltuu tosin vain toimialoille, joissa asiakasvaatimukset ja luottamus toimittajan tietoturvallisuuteen ovat tärkeitä menestystekijöitä. Luottamusta muistuttavia mittareita löydettiin muutama. Jaquith (2007, s. 280) esitti mittariksi asiakkaan arvioita yrityksen tietoturvallisuuden suorituskyvystä ja Savola (2007) mainitsi luottamuksen mittaamisen osan ylimmän johdon mittaristoa, muttei kuvaillut esimerkkimittareita. Kujansivu et al. (2007, s. 179) taas ehdottavat mittariaihioiksi ”asiakassuhteen keskimääräinen kesto” ja ”menetettyjen tärkeiden asiakkaiden osuus kaikista asiakkaista”, joilla mitataan asiakasuskollisuutta. Nämä mittariaihiot liittyvät läheisesti myös luottamukseen. Luottamuksen väheneminen voi ennustaa esiesimerkiksi asiakassuhteiden lyhentymistä tai asiakkaan menetystä. Kuten luvussa 2.3.3 mainittiin, tietoturvallisuuden mittaaminen on läheisesti sidoksissa aineettoman pääoman mittaamiseen ja osa tietojohtamisen tasoa kuvailevaa mittaamista.

Kujansivu et al. (2007, s. 180-181) esittelevät prosessien toimivuutta kuvailevia mittareita. Tällaisia ovat esimerkiksi itsearvioinnit ja auditoinnit sekä dokumentoitujen järjestelmien määrä. Kriittisten järjestelmien tunnistaminen ja tuotekohtainen tietoturvasuunnitelma ovat periaatteeltaan tällaisia prosessia kuvaavia mittareita ja ne kuvailevat tietoturvallisuuden toimivuutta prosessien ohessa. Tuotekohtainen tietoturvasuunnitelma on kunnianhimoinen mittari, jonka avulla tavoitellaan hyvin hallinnoidun ja toteutetun tietoturvatoiminnan todistamisella asiakasvaatimuksilta välttymistä. Kriittisten järjestelmien tunnistaminen taas tukee sisäisiä prosesseja ja tietoturvapäällikön työtä. Laadun mittaaminen on hyvin samankaltainen mittari, kuin Kujansivun et al. (2007, s. 181) esittelemä mittariaihio ”automatisoitujen prosessien osuus”, joka kuvastaa kuinka hyvin teknologiaa osataan hyödyntää liiketoiminnan tukena. Loppujen lopuksi tietoturvallisuuden mittaamisella pyritään selvittämään ja osoittamaan, kuinka hyvin tietoturvatoiminta tukee liiketoiminnan tavoitteita ja kuinka hyvin tietoturvallisuus on onnistuttu huomi-

oimaan osana liiketoimintaa. Holistisen tason mittarit ovat samankaltaisia kuin tietojohtamisen ja yleisen liiketoiminnan mittarit.

7 PÄÄTELMÄT

Tutkimuksen tavoitteena oli tunnistaa tapoja mitata tietoturvallisuutta siten, että mittaamisen avulla voidaan ymmärtää tietoturvallisuuden tila ja hallinnoida sitä tietoturvastrategian mukaisesti. Tätä varten kartoitettiin, mitä tietoturvallisuuteen liittyviä tietotarpeita kohdeyrityksen ylimmällä johdolla ja tietoturvapäälliköllä on tietoturvallisuuteen liittyen ja etsittiin parhaiten kohdeyrityksen tietoturvallisuuden tilaa kuvaavia menestystekijöitä. Tutkimuksen teoriaosuus käsittelee tietoturvallisuuden ja mittaamisen kirjallisuutta, sekä muodostaa viitekehyksen mittaristoprojektille. Empiirinen osuus taas perustuu toimintatutkimukseen, jonka tueksi kerättiin aineistoa teemahaastattelulla. Toimintatutkimuksen prosessin aikana muodostettu mittaristo esiteltiin kohdeyritykselle ja sen arvio perustuu avoimeen haastatteluun.

Tämän luvun aluksi tarkastellaan tutkimuksen tuloksia ja vastataan tutkimuskysymyksiin sekä toteutetaan toimintatutkimuksen prosessin viimeinen vaihe, tieteellinen arviointi. Muodostettujen johtopäätösten perusteella esitetään toimintasuositukset kohdeyritykselle. Lopuksi arvioidaan toimintatutkimuksen onnistumista sekä pohditaan mahdollisia jatkotutkimusaiheita.

7.1 Tutkimuksen johtopäätökset

Tutkimuksen päätutkimuskysymykseksi asetettiin ”*Miten yrityksen tietoturvallisuutta voidaan mitata niin, että mittaamisen avulla ymmärretään tietoturvallisuuden tila ja voidaan hallinnoida sitä tietoturvastrategian mukaisesti?”*. Tähän kysymykseen haettiin vastauksia neljällä apukysymyksellä, joihin löydettiin vastauksia sekä teoriaosuudesta että empiriasta. Tutkimuksen johtopäätökset muodostuvat löydettyjen vastausten yhteenvedosta.

Ensimmäinen alatutkimuskysymys oli: *Mitä tietoturvallisuus tarkoittaa osana liiketoimintaa ja mitä haasteita sen mittaamisessa on?* Tätä kysymystä tarkasteltiin tutkimuksen teoriaosassa luvussa 2, jossa tietoturvallisuus määriteltiin käsitteenä ja pohdittiin miten se liittyy organisaation toimintaan. Tietoturvallisuus on liiketoiminnalle tukifunktio, jota tulee hallinnoida liiketoiminnan vaatimukset ja tarpeet huomioiden. Toisaalta tietoturvallisuudella on tärkeä rooli organisaation jokaisen toiminnon ohessa niiden keräämien ja käyttämien tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaamisessa. Tietoturvallisuus pyrkii estämään organisaation tietoon liittyviä epäsuotuisia tapahtumia ja varmistamaan, että oikea tieto saavuttaa oikean henkilön tai laitteen oikeassa paikassa oikeaan aikaan. Tämä tarkoittaa laajimmillaan yrityksen toimintakyvyn

varmistamista, sillä tiedon merkitys liiketoiminnan sujuvuudelle on huomattavan suuri. Tietoturvallisuutta ei siis voida jättää yksittäiseksi toiminnoksi, vaan se tulee huomioida liiketoimintaprosessien yhteydessä, liiketoimintajohtamisessa ja riskien hallinnassa. Johtoryhmätasolla tärkeimmät tehtävät ovat määrittää liiketoiminnalle sopiva riskitaso sekä varmistaa, että tietoturvallisuus on järjestetty organisaation tavoitteiden mukaisesti ja tarjota riittävät resurssit sen hallinnoimiseksi. Liiketoiminnan edustajien on myös asetettava tavoitteita, joiden kautta ilmaistaan vastuu tietoturvaorganisaatiolle, joka liiketoiminnan tarjoamien resurssien puitteissa hallinnoi tietoturvallisuutta ja siihen liittyviä riskejä. Tietoturvallisuuden ylläpitäminen sekä tietoturvatapahtumien ja riskien havaitseminen on kuitenkin jokaisen työntekijän vastuulla. Tietoturvamittareiden avulla voidaan osoittaa, kuinka hyvin johdon asettamat tavoitteet toteutuvat käytännössä, ohjata henkilöstöä toimimaan tavoitteiden mukaisesti, havaita ongelmia ja ymmärtää mikä liiketoiminnan näkökulmasta on tärkeää tietoturvallisuudelle

Koska tietoturvallisuus on käsitteenä laaja ja tietoturvavaatimukset muuttuvat jatkuvasti, on tavoitteiden asettaminen haastavaa. Tästä syystä myös tietoturvallisuuden mittaaminen liiketoiminnan näkökulmasta on haastavaa. Esimerkiksi tämän tutkimuksen kohdeyrityksessä ei ole asetettu koko yrityksen kattavaa tavoitetta tietoturvallisuudelle eikä siitä raportoida säännöllisesti. Ilman säännöllistä raportointia mittarit ovat hyödyttömiä, koska niiden perusteella ei voida tehdä päätöksiä, jos ne eivät tavoita kohdeyleisöään. Tietoturvallisuudelle osoitetut resurssit ovat usein pienet eikä erillistä budjettia ole välttämättä muodostettua tietoturvallisuuden kehittämistä varten. Resurssien puuttumisen vuoksi mittaamista on haastava toteuttaa käytännössä. Mikäli mittarit toteutettaisiin, tulisi niiden reliabiliteetin ja validiteetin olla todella hyvällä tasolla, jotta ne eivät anna johdolle väärää mielikuvaa tietoturvallisuuden tilasta. Tietoturvallisuuden mittaamisen haasteena onkin, että sitä saatetaan suorittaa väärin painotuksin, liian suppeasti tai ei osata sanoa mitä oikeasti mitataan ja mitä mittaustulos lopulta kertoo tietoturvallisuudesta. Väärien mittaustulosten perusteella henkilöstöä saatetaan ohjata toimimaan tietoturvallisuuden tilaa heikentävästi tai kohdistaa liikaa resursseja asioihin, joiden merkitys liiketoiminnalle on minimaalinen. Esimerkiksi vaatimustenmukaisuutta voidaan mitata sen perusteella, kuinka suuri osa vaatimuksista pystytään täyttämään. Lopullinen näkemys siitä, täytetäänkö vaatimusta vai ei, on täysin subjektiivinen. Tämänkaltainen mittari voi antaa hyvän kuvan vaatimustenmukaisuudesta, vaikka käytännöntasolla toiminta ei täysin vastaisikaan vaatimuksia. Tällöin mittareiden avulla muodostettu arvio käytännön toiminnasta on virheellinen eikä mahdollisia ongelmia pystytä havaitsemaan, jolloin tavoitteiden asettaminen ja toiminnan ohjaaminen mittareiden perusteella ei ole relevanttia. Usein tietoturvallisuuden mittaamisen ongelmana onkin, että siihen liittyvistä asioista on haastavaa saada objektiivista ja yksiselitteistä tietoa. Tärkeimmät tässä tutkimuksessa havaitut haasteet tietoturvallisuuden mittaamisessa ovat:

- Tietoturvallisuus on laaja ala, johon liittyvät vaatimukset muuttuvat jatkuvasti
- Tietoturvallisuudesta ei raportoida formaalisti, jolloin mittarit eivät saavuta kohdeyleisöään

- Tietoturvallisuuden hallinnoinnille ei ole asetettu tavoitteita, joiden perusteella mittarit voitaisiin muodostaa
- Tietoturvaorganisaation resurssit eivät riitä mittariston muodostamiseen
- Mittariston vaarana on osaoptimointi, jolloin tietoturvallisuutta ei hallinnoida riittävän kattavasti
- Tietoturvallisuudesta on haastava saada objektiivista tietoa
- Mittaamisella ei ole liiketoimintajohdon tukea

Toinen alatutkimuskysymys oli: *Miksi kohdeyrityksen tietoturvallisuutta mitattaisiin ja mitä tietotarpeita eri johtotasoilla on tietoturvallisuuden suhteen?* Tätä kysymystä käsiteltiin yleisesti liiketoiminnan mittaamisen liittyen luvussa 3.2 ja tietoturvallisuuden näkökulmasta luvussa 4.3. Kirjallisuuden mukaan tietoturvallisuuden mittaaminen voidaan perustella samalla tavalla kuin liiketoiminnan mittaaminen yleisesti perustellaan. Mittaamisen avulla voidaan tukea strategian konkretisointia ja ohjata toimintaa sen mukaisesti. Toiminnan ongelmat voidaan havaita mittaamisen avulla ja mittareiden kautta on mahdollista ymmärtää organisaation toiminnan vaikutuksia esimerkiksi myyntiin tai tuotannon tehokkuuteen. Tietoturvallisuuden mittaaminen on ajankohtainen aihe, sillä tietoturvallisuuteen liittyvät uhat ovat lisääntyneet ja tieto on usein liiketoiminnalle kriittinen kilpailutekijä. Tietoturvallisuutta mittaamalla on mahdollista arvioida tietoriskejä, ymmärtää tietoturvallisuuden suorituskyky ja varmistaa että liiketoiminnan jatkumista edesauttavat tietoturvatoiminnot ovat tavoitteiden mukaisia. Lisäksi mittareiden kautta voidaan asettaa tavoitteita tietoturvallisuudelle ja ohjata henkilöstöä toimimaan niiden mukaisesti. Tärkeää on myös osoittaa läpinäkyvyyttä sidosryhmille, joilta tietoturvavaatimukset usein tulevat. Nämä syyt mittaamiselle tulivat esille myös kohdeyrityksessä suoritetuissa haastatteluissa. Yksi tärkeimmistä kohdeyrityksen tavoitteista on osoittaa mittaamisen avulla tietoturvallisuuden taso ja siten pyrkiä ennakoivasti vastaamaan asiakasvaatimuksiin ja osoittamaan tämä mittareiden avulla. Hyvin toteutettujen mittareiden tuloksia voisi olla mahdollista käyttää myös myynnin tukena. Kohdeyrityksen sisäisen toiminnan näkökulmasta tavoitteena olisi ymmärtää tuotteisiin ja niiden kehittämiseen sekä sisäisiin prosesseihin ja järjestelmiin liittyvä tietoturvallisuus holistisella tasolla. Kun näiden lisäksi motivaationa mittaamiselle on tavoitteiden asettaminen ja toiminnan ohjaaminen mittareiden perusteella, voidaan tietoturvallisuuden mittaamista pitää kommunikointivälineenä. Tietoturvallisuutta kannattaa mitata, koska mittaustulosten kautta voidaan selvittää tietoturvallisuuden tila ja kommunikoida se liiketoimintajohdolle, joka asettaa mittareihin liittyviä tavoitteita tietoturvatoiminnalle. Tärkeimmät tässä tutkimuksessa havaitut syyt mitata tietoturvallisuutta ovat:

- Tietoturvallisuuden hallinnointiin liittyvän päätöksenteon tuki
- Läpinäkyvyyden osoittaminen sidosryhmille
- Vaatimustenmukaisuuden varmistaminen
- Syy-seuraus suhteiden ymmärtäminen

- Tietoturvallisuudesta kommunikointi ja tietoturvatietoisuuden lisääminen
- Tietoturvatoiminnan ohjaaminen ja kehittymisen seuraaminen
- Ongelmien ja riskien havaitseminen
- Tietoturvallisuuden liittäminen liiketoimintaprosesseihin
- Tarve yhtenäiselle näkemykselle tietoturvallisuuden tilasta

Kirjallisuudesta löydettiin johdon näkökulma tietoturvallisuuteen, joka esitellään luvussa 2.3.1. Korkeimmilla johtotasoilla tietotarpeet tietoturvallisuudesta liittyvät rahaan ja tietoturvallisuuden tilaan kokonaisuudessaan. Liiketoimintajohtajat tarvitsevat edellä mainittujen tietojen lisäksi tietoa tietoturvallisuuden suorituskyvystä, eli siitä miten tietoturvallisuus vastaa sille asetettuihin tavoitteisiin suunnitellulla tavalla. Kohdeyrityksessä johtoryhmä näkee tietoturvallisuuden asiakkaan näkökulmasta laadun ja tietoriskien kautta. Johtoryhmää kiinnostaa, miten asiakasvaatimuksiin pystytään vastaamaan hyvän laadun ja tietoturvallisten prosessien kautta. Toisaalta kohdeyrityksen johtoryhmälle on tärkeää, että asiakkaiden asettamiin tietoturvavaatimuksiin vastataan kustannustehokkaasti. Seuraavalla johtotasolla tietotarpeet liittyvät asiakkaiden kanssa sovittujen palvelutasojen käytännön toteutukseen ja yksityiskohtaisempiin asioihin, kuten kapasiteetinhallintaan ja tietoturvatapahtumiin. Tietoturvapäällikön tietotarpeet liittyvät vahvasti johtoryhmän asettamiin tavoitteisiin. Tavoitteiden avulla tietoturvapäällikkö pystyy kohdistamaan käytössä olevia resursseja tehokkaammin ja hallinnoimaan kohdeyrityksen tietoturvallisuutta liiketoiminnan tarpeiden mukaisesti. Lisäksi tietoturvapäällikkö tarvitsee yksityiskohtaista tietoa tietoturvatapahtumista sekä siitä kuinka hyvin niitä osataan havainnoida ja miten niihin käytännössä reagoidaan.

Kirjallisuustutkimuksessa liiketoimintajohtajien näkökulmaan olisi voitu saada lisää syvyyttä tutkimalla liiketoimintajohtamista, sillä lähtökohdat tietoturvallisuuden mittaamiselle ovat täysin samat kuin liiketoiminnan mittaamisessa. Toisaalta tämän tutkimuksen löytönä voidaan pitää, että tietoturvallisuus on yksi liiketoimintaan liittyvä funktio, jonka kautta on mahdollista tuottaa lisäarvoa asiakkaille tietyillä toimialoilla. Niillä toimialoilla, joissa tietoturvallisuuden kautta ei voida tuoda lisäarvoa asiakkaalle, mittaamista tulee pohtia eri näkökulmasta. Lähtökohtaisesti ylimmän johdon tietotarpeet liittyvät toimialan liiketoimintaa ohjaaviin tekijöihin ja sidosryhmien vaatimuksiin. Näitä ovat esimerkiksi lainsäädäntö, alan standardit, raha ja liiketoimintatietoon liittyvät riskit. Voidaan myös olettaa tämän tutkimuksen kohdeyrityksen johdon näkemyksen siitä, että tietoturvallisuus liittyy läheisesti laadun ylläpitämiseen ja kehittämiseen, olevan yleistettävissä myös muille toimialoille. Tämä tarkoittaa sitä, että liiketoimintajohdon tietotarpeena on yleisesti toiminnan laadun tila, jossa huomioidaan myös tietoturvallisuuden tila. Liiketoimintajohdon ei ole tarpeen tietää yksityiskohtaisia kuvauksia tietoturvallisuudesta, vaan varmistaa onko heidän tietotarpeisiin liittyvät asiat tietoturvallisuuden kannalta kunnossa ja minne tämän perustella pitää investoida. Alemmille johtotasoille mentäessä tietotarpeet liittyvät prosessien toimivuuteen ja operatiivisen toiminnan hallintaan, joiden tavoitteet muodostuvat liiketoimintaa ohjaavista tekijöistä.

Tietoturvallisuuteen liittyvistä tietotarpeista muodostuu menestystekijöitä, jotka listataan seuraavan vastauksen yhteydessä.

Kolmanneksi alatutkimuskysymykseksi asetettiin: *Mitkä menestystekijät kuvailevat kohdeyrityksen tietoturvallisuuden tilaa parhaiten?* Tähän tutkimuskysymykseen vastattiin kattavasti luvussa 6.2. Luvussa 3.3 esitellyn tasapainotetun tuloskortin avulla vastauksia pystyttiin ymmärtämään paremmin liiketoiminnan viitekehyksessä. Menestystekijät, kuten palvelutaso, luottamus, laatu, tietoturvatapahtumat ja tietoriskit, pystyttiin tasapainotetun tuloskortin avulla liittämään liiketoimintaan. Lisäksi menestystekijöiden välisiä suhteita esiteltiin luvussa 3.3, jossa hahmoteltiin miten palvelun laatu liittyy asiakasuskollisuuteen, joka taas on läheisesti sidoksissa kannattavuuteen. Palvelun laatua taas tukee osaaminen, joka kohdeyrityksessä nähtiin tärkeänä yleisesti sisäisessä tietoturvatoiminnassa ja varsinkin tuotekehityksessä. Tuotteiden ja palvelujen tietoturvallisuus voidaan nähdä korkean tason menestystekijänä, jota voidaan tukea työntekijöiden osaamisella, standardisoiduilla prosesseilla ja monipuolisella testauksella. Toinen korkean tason menestystekijä kohdeyrityksen tietoturvallisuudelle on se, kuinka hyvin yrityksen toimintaan liittyvä tietoturvallisuus ymmärretään kokonaisvaltaisesti. Tähän liittyy olennaisesti kyky tunnistaa tietoriskejä, kriittisiä järjestelmiä ja yleisemmin tietoturvallisuutta liiketoimintalinjoissa. Toimintaympäristön näkökulmasta olennainen menestystekijä on sijoitus toimialavertailussa, sillä sen avulla voidaan esimerkiksi lisätä asiakkaiden luottamusta kohdeyritykseen. Tärkeimmät tässä tutkimuksessa havaitut tietoturvallisuuden menestystekijät ovat:

- Kokonaisvaltainen ymmärrys yrityksen tietoturvallisuudesta
- Kyky havaita tietoriskejä ja reagoida niihin
- Kyky havaita tietoturvatapahtumia ja reagoida niihin
- Kyky tuottaa tietoturvallisia tuotteita ja palveluita
- Kyky täyttää sidosryhmien vaatimukset
- Tietoturvallisuus osana laatua
- Kustannustehokkuus
- Palvelutaso
- Luottamus sidosryhmissä
- Menestys toimialavertailussa

Kaiken kaikkiaan luvussa 6.3 esitetty viitekehys mittaristolle kokoaa nämä asiat yhteen ja liittää ne johdon esittämiin näkökulmiin, joista tietoturvallisuutta halutaan tarkastella. Johtoryhmätason tietotarpeet tiivistetään neljään mittausteemaan, kun taas niihin liitettävät mittarit vastaavat muiden operatiivisenjohdon ja tietoturvajohdon tietotarpeisiin. Näistä mittareista on mahdollista koostaa raportti johtoryhmälle, joka vastaa heidän tietotarpeisiin.

Neljäs, ja lopputulosten esittämisen kannalta tärkein, alatutkimuskysymys oli ”*Miten kohdeyrityksen tietoturvallisuutta voidaan mitata?”*. Tähän kysymykseen voidaan vastata kaksiosaisesti. Ensinnäkin mittaristoprojektin tukena käytetyt haastattelut ovat kokonaisuudessaan keino mitata subjektiivisesti kohdeyrityksen tietoturvallisuutta holistisella tasolla. Teemahaastattelujen avulla kerättyä aineistoa analysoimalla voidaan periaatteessa päätellä, mikä on kohdeyrityksen tietoturvallisuuden tila ja ymmärtää siihen vaikuttavat tekijät. Tätä varten kysymysrunkoa tulisi muuttaa hieman yksityiskohtaisemmaksi ja suorittaa laajempi haastattelukierros, jolloin kyseessä on tietoturva-auditointi. Tietoturvallisuuden tilaa ei kuitenkaan pystytä selvittämään kysymällä suoraan mikä on tietoturvallisuuden tila, sillä vastaukset vaihtelevat huomattavasti riippuen vastaajan näkökulmasta. Esimerkiksi tässä tutkimuksissa haastatelluilta kysyttiin, mikä heiden mielestään on kohdeyrityksen tietoturvallisuuden tila asteikolla 1-10. Vastaukset vaihtelivat 3 ja 8,5 välillä, josta voidaan päätellä että yhteinen näkökulma tietoturvallisuuteen puuttuu ja tietoturvallisuuden tilan arviointiperusta on erilainen. Yhteisen arviointiperustan muodostaminen yhdessä tietoturvatavoitteiden kanssa on hyvä lähtökohta mittaamiselle. Viitekehys arviointiperustalle muodostettiin tässä tutkimuksessa tasapainotettua tuloskorttia mukaillen, jonka kautta esitellään mitkä asiat tietoturvallisuuteen vaikuttavat ja johon tietoturvamittarit liitetään.

Toinen vastaus siihen, miten tietoturvallisuutta voidaan mitata, on mittaristo joka esitellään luvussa 6.3. Mittaristossa huomioidaan haastattelujen avulla löydetyt menestystekijät, jotka kuvailevat kohdeyrityksen tietoturvallisuutta ja pyrkivät vastaamaan haastatteluissa esiin tulleisiin tietotarpeisiin. Mittariston avulla kohdeyrityksen tietoturvallisuutta voidaan tarkastella holistisella tasolla ja sen avulla voidaan arvioida, miten tietoturvallisuus liittyy kohdeyrityksen liiketoimintaan. Mittariston viitekehystä voidaan käyttää myös muissa yrityksissä, mutta siihen liitettävät mittaamisteemat on muodostettava läheisessä yhteistyössä johtoryhmän ja liiketoiminnan edustajien kanssa. Tässä tutkimuksessa käytetty mittaristoprojekti soveltuu keinoksi muodostaa mittaristo, jolla erilaiset yritykset eri toimialoilla voivat mitata tietoturvallisuuttaan liiketoiminnan näkökulmasta. Mittaristoprojekti on toisaalta myös yleisluontoinen keino toteuttaa liiketoiminnan tarpeisiin vastaava mittaristo, koska sen tarkoituksena on selvittää mittaamistarpeita yhteistyössä ylimmän johdon kanssa. Tästä syystä voidaankin olettaa että tässä tutkimuksessa suunniteltuun mittaristoon liitetyt mittaamisteemat ovat yleisesti hyödyllisiä lähtökohtia yrityskohtaisten mittareiden valintaan. Tätä oletusta tukee esimerkiksi alkuperäisen tasapainotetun mittariston ajatus siitä, että sisäisen toiminnan kautta voidaan vaikuttaa asiakasnäkökulmaan, joka puolestaan vaikuttaa suoraan liiketoimintaan.

Vastaus päätutkimuskysymykseen muodostuu apukysymysten kautta. Ensinnäkin mittaajan tulee ymmärtää, mikä on tietoturvallisuuden rooli yrityksen liiketoiminnalle. Tämä voidaan selvittää esimerkiksi haastattelemalla liiketoimintajohtoa, jolloin voidaan hahmottaa mitkä asiat vaikuttavat yrityksen tietoturvallisuuteen. Tässä yhteydessä myös johdon tulee olla riittävän motivoitunut tietoturvallisuuden mittaamiseen, jotta mittaa-

mista pystytään suorittamaan. Haastatteluissa selvitetään siis tietoturvastrategia, pyritään saavuttamaan johdon tuki mittaamiselle ja asetetaan tavoitteita tietoturvallisuuden hallinnoinnille. Tämän jälkeen tulee pohtia, mitä tietotarpeita liiketoimintajohdolla on tietoturvallisuuteen liittyen. Haastatteluja analysoimalla löydetään tietotarpeisiin liittyviä menestystekijöitä, joissa yrityksen sisäisessä toiminnassa tulee onnistua. Menestystekijöihin voidaan liittää mittareita, jotka kuvailevat niihin liittyvän tietoturvatoiminnan onnistumista. Todennäköisemmin tietoturvamittari kuitenkin kuvailee kuinka hyvin tietoturvatoiminta kehittyy kohti tavoiteltua tasoa ja yrityksen kykyä havaita tietoturvallisuuteen vaikuttavia tapahtumia. Tämä tarkoittaa esimerkiksi sitä, että yritys oppii ymmärtämään, mitkä järjestelmät ovat kriittisiä yrityksen tietoturvallisuuden kannalta ja kuinka hyvin tietoturvatapahtumiin pystytään reagoimaan. Tietoturvan hallinnointi strategian mukaisesti tarkoittaa lopulta sitä, että mittaustulosten perusteella voidaan nähdä miten tietoturvallisuus kehittyy kohti tavoitetilaa ja käyttää sen mukaisesti resursseja kohteisiin, joiden kehittymistä halutaan tukea. Mittaustulosten kautta voidaan asettaa tavoitteita, joilla käytännön toimintaa ohjataan toimimaan tietoturvastrategian mukaisesti.

Tämän tutkimuksen lopputuloksena on, että tietoturvallisuutta voidaan hallinnoida tietoturvastrategian mukaisesti mittaamalla sitä, miten tietoturvallisuutta onnistutaan kehittämään ja toteuttamaan tavoitteiden mukaisesti. Tuloksena voidaan pitää myös sitä, että liiketoimintalähtöisen mittaamisen tulee perustua sidosryhmien vaatimuksiin, joista myös tietoturvastrategia muodostuu. Kirjallisuusselvityksessä ei löydetty tietoturvamittareita, jotka olisi osoitettu suoraan liiketoimintajohdolle ja joiden kautta tietoturvapäällikölle voidaan osoittaa tavoitteita tietoturvallisuuden hallinnoinnille. Selkeä viesti kuitenkin on, että myös tällaisille mittareille on tarvetta. Esimerkiksi Savola (2007) esittelee liiketoiminnalle suunnattujen tietoturvamittareiden olevan taloudellisia, luottamusta arvoketjussa osoittavia, liiketoimintatason tietoriskejä kuvailevia tai järjestelmätason tietoturvallisuuden suorituskykyä mittaavia. Käytännön esimerkkejä näistä ei kuitenkaan annettu. Brotby (2009) mainitsee, että tasapainotetun mittariston käyttäminen on tietoturvallisuuden hallinnoinnin kannalta paras vaihtoehto, muttei anna käytännön esimerkkejä siihen, mitä osa-alueita mittaristo sisältäisi. Lähimpänä tämän tutkimuksen lopputulosta, joka esitetään Kaplanin & Nortonin (2004) esittelemästä tasapainotetusta tuloskortista sovelletun viitekehyksen avulla, on Jaquith (2007) joka esittelee tasapainotetun mittaristo ja siihen liittyviä mittareita. Jaquithin ratkaisussa on kuitenkin kaksi ongelmaa, joihin tämä tutkimus tuo ratkaisuja. Ensinnäkin Jaquithin tasapainotettu mittaristo muodostuu teknispainotteisesti, jolloin mittarit eivät tuo lisäarvoa liiketoimintajohdolle, koska ne ovat liian yksityiskohtaisia eivätkä ne huomioi liiketoimintaprosesseja, joihin ne voitaisiin liittää. Toisaalta mittaristossa ei huomioida eikä mainita liiketoimintajohtoa tai pohdita, miksi eri mittarit olisivat tärkeitä liiketoiminnalle.

Tämä tutkimus tuo lisäarvoa tietoturvallisuuden mittaamisen tutkimukselle huomioimalla liiketoiminnan tarpeet ja perustelemalla, miksi valitut mittarit olisi syytä ottaa käyt-

töön. Vaikka tutkimuksen tuloksissa esitellään vain kymmenen mittaria, on ne perusteltu ja kuvailtu tarkasti, mikä lisää sekä mahdollisuuksia niiden käyttöönottoon että todennäköisyyttä sille, että ne mittaavat ja kuvailevat liiketoimintalähtöisesti tietoturvallisuuden tilaa. Mittarit vastaavat myös Savolan (2007) esittelemään jaotteluun liiketoiminnan tietoturvamittareista. Lisäksi pystyttiin tunnistamaan tietoturvallisuuden menestystekijöitä, joiden hahmottaminen kirjallisuustutkimuksen avulla oli haastavaa. Mittaamisen teoriaan tämä tutkimus ei tuo lisäarvoa, vaikkakin suunniteltua mittaristoprojektia ja viitekehystä mittaristolle voidaan käyttää myös yleisesti mittariston suunnitteluun ja mittareiden valintaan. Mittaamisen tutkimuksia, kuten Bournea et al. (2000), Neelya et al. (2000), Lönnqvistiä et al. (2006), Kujansivua et al. (2007) ja Ylisirniöä (2011) hyödynnettiin ymmärtämään, mitä mittaaminen tarkoittaa osana johtamista ja miten mittaristo voidaan suunnitella. Tämä toi todella paljon lisäarvoa, ymmärrystä ja liiketoimintalähtöisyyttä tietoturvamittariston suunnitteluun ja mittareiden valintaan.

7.2 Suositukset kohdeyritykselle

Tämän tutkimuksen perusteella kohdeyritykselle suositellaan mittariston käyttöönottoa. Tutkimuksessa löydettiin selkeä perustelu sille, että tietoturvallisuuden mittaaminen nähdään tärkeänä kohdeyrityksessä, vaikka johto oli haluton esittämään arvioitaan mittariston onnistumisesta. Mittaamisen avulla voidaan tukea päätöksentekoa sekä viestiä koko yrityksen kattavia tavoitteita ja jakaa vastuita tietoturvallisuuden toteuttamisesta. Lisäksi mittariston avulla pystytään kehittymään riskienhallinnassa ja ymmärtämää entistä paremmin, miten tietoturvallisuus liittyy eri liiketoimintalinjojen toimintaan. Asiakasnäkökulman mittaaminen on tärkeää, sillä hyvän luottamuksen ja palvelutason ylläpitäminen ovat kriittisiä menestystekijöitä kohdeyrityksen toiminnalle. Sisäisen toiminnan tietoturvallisuuden mittaaminen taas antaa tietoturvapäällikölle näkemyksen siitä, mihin resursseja halutaan kohdista.

Mittaamisen käyttöönoton onnistumiseksi johtoryhmän tulisi sitoutua läheisemmin tietoturvallisuuden kehittämiseen. Tämä tarkoittaa esimerkiksi koko yrityksen kattavien tavoitteiden asettamista siitä, mihin tietoturvallisuudella ja sen mittaamisella pyritään. Tavoitteet tukevat ensinnäkin mittaamista, mutta antavat myös koko henkilöstölle selkeän näkemyksen siitä, mikä on tietoturvallisuuden näkökulmasta tärkeää kohdeyritykselle. Tavoitteita tulee muodostaa tietoturvamittaristoon liittyen, jotta sitä voidaan hyödyntää osana tietoturvallisuuden hallinnointia. Hallinnointia voidaan tehdä läpinäkyvämmäksi ja liiketoimintalähtöiseksi formaalin tietoturvaraportoinnin avulla, jossa mittaustulosten ohella kuvaillaan niihin vaikuttavia tekijöitä. Formaalit raportointikäytännöt tulee siis muodostaa sekä mittareiden tulosten viestimistä varten sekä tehokkaan liiketoiminnan ja tietoturvaorganisaation välisen kommunikoinnin tueksi. Tavoitteita voidaan tarkentaa mittareista saatujen käyttökokemusten perusteella. Mittariston arviointi ja ylläpito tulisikin huomioida esimerkiksi liiketoimintaan liittyvien muutosten yhteydessä ja jatkuvana osana tietoturvallisuuden hallinnointia. Mittariston arvioinnin

yhteydessä voidaan suunnitella yksityiskohtaisempia mittareita, muokata mittareita muuttuneiden tavoitteiden mukaisiksi ja poistaa tarpeettomia mittareita käytöstä.

Mittaamista ei ole tule toteuttaa erillisenä toimenpiteenä, vaan se tulee liittää mahdollisimman tiiviiksi osaksi olemassa olevaa toimintaa. Esimerkiksi luottamusta voi mitata muiden asiakaskyselyiden yhteydessä, palvelutasosopimuksia osana myyntiprosessia ja huoltokatkoja muun palvelutason mittaamisen ohella. On myös mittareita, jotka vaativat prosessin tunnistamisen ja kuvaamisen. Esimerkiksi tuotekohtaisen tietoturvasuunnitelman toteuttamiseksi sekä tuoteprosessi että siihen vaikuttavat tietoturvavaatimukset on tunnettava tarkasti. Tietoturvatapahtumien mittaaminen taas yrityslaajuisen motivaatioon ja mahdollisimman yhteisen näkemyksen siitä, mitä ovat tietoturvatapahtumat ja miten niiden vakavuutta arvioidaan. Mittaamiseen liittyvillä tavoitteiden ja vastuiden asettamisella ja käyttöönottoon liittyvillä valmisteluilla varmistetaan, että kohdeyrityksellä on kyky reagoida mittareiden osoittamiin tuloksiin ja yhteinen ymmärrys siitä, mitä tulokset tarkoittavat.

Kohdeyrityksen toiminnan kannalta on tärkeää tarjota tukea ja toimintaohjeita tuotepäälliköille, joille on siirretty vastuuta tietoturvallisuudesta. Tämä voidaan tehdä tuotekohtaisen tietoturvasuunnitelman avulla, mutta myös kouluttaminen on tässä yhteydessä suositeltavaa. Tuotekohtaiset tietoturvasuunnitelmat tulisi muodostaa läheisessä yhteistyössä tuotepäälliköiden kanssa siten, että tietoturva-asiantuntijat muodostavat viitekehyksen tuotteisiin liittyvistä tietoturvavaatimuksista, joiden kriittisyyden ja tavoitteet liiketoiminnan edustaja määrittää. Tuotteisiin liittyvien tietoturvavastuiden lisäksi olisi suositeltavaa osoittaa koko henkilöstön vastuu tietoturvatapahtumien havainnoinnista ja ongelmien esiintuomisesta. Usein subjektiivinen ja käytännönläheinen näkemys siitä, mitä ongelmia tietoturvallisuudessa on, muodostaa kattavan kuvan tietoturvallisuuden tilan heikoista lenkeistä ja tukee sen hallinnointia.

7.3 Tutkimuksen tarkastelu

Tieteellisen tutkimuksen onnistumista ja suorittamista tarkastellaan perinteisesti reliabiliteetin ja validiteetin käsitteiden kautta (Olkkonen 1993, s. 38-39; Yin 2003, s. 34-36; Koskinen et al. 2005, s. 254-255). Reliabiliteetilla tarkoitetaan sitä, kuinka hyvin tutkimussuoritus voidaan toistaa käytetyillä menetelmillä. Validiteetti taas kuvailee kuinka hyvin käytetyt menetelmät soveltuvat kohteena olevan ilmiön tutkimiseen. Validiteetin ja reliabiliteetin avulla arvioidaan perinteisesti määrällisiä tutkimuksia. Niiden avulla suoritettua laadullisen tutkimuksen tarkastelua voidaan tästä syytä kritisoida, sillä tutkimuksen tulokset ovat subjektiivisia. (Olkkonen 1993, s. 38-39; Yin 2003, s. 35-37; Koskinen et al. 2005, s. 254-256.) . Reliabiliteetin ja validiteetin lisäksi tutkimusta voidaan Gummessonin (2000, s. 185) mukaan arvioida myös sen mukaan, kuinka hyvin tutkimuksen tuloksia voidaan yleistää tapaustutkimuksen ulkopuolelle ja kuinka uskottava tutkimus on. Susmanin & Everdin (1978) mukaan toimintatutkimuksen tieteelli-

syyttä on relevanttia tarkastella määrällisen tutkimuksen tarkastelun avulla, mutta tuloksia pikemminkin tutkimuksen kohteen näkökulmasta. Tämän toimintatutkimuksen tuloksia kohdeyrityksen näkökulmasta arvioitiin luvussa 6.4

Tutkimuksen reliabiliteettia kasvattaa siinä käytettyjen menetelmien kattava kuvaaminen, joka tukee myös tutkimuksen uskottavuutta. Esimerkiksi teemahaastattelu on mahdollista toistaa, vaikkakin sen puolistrukturoitu rakenne heikentää tutkimuksen reliabiliteettia. Teemahaastattelussa tutkijan esittämät tarkentavat lisäkysymykset ja kyky johdatella haastateltavaa vastaamaan kysymyksiin mahdollisimman syvällisesti saattavat johtaa hyvinkin erilaisiin vastauksiin ja siten erilaiseen aineistoon. Voidaan kuitenkin aihepiirin rajauksen ja teemojen selkeyden vuoksi olettaa, että samat asiat olisivat nousseet haastattelussa esille, vaikka haastattelun olisi suorittanut toinen tutkija. Haastattelujen jälkeen niissä esiin tulleet aiheet voidaan löytää myös toisen tutkijan toimesta, sillä käytetty aineiston analyysimenetelmä on kuvailtu tarkasti. Voidaan myös pohtia, ymmärsivätkö kaikki haastatellut kysymykset samalla tavalla. Tietoturvallisuudesta puhuttaessa päädyttiinkin haastatellusta riippuen esimerkiksi sopimuksiin ja niiden tuomiin tietoturvavelvoitteisiin tai hyvin tietoteknisiin asioihin. Tämä osalta reliabiliteettia pyrittiin parantamaan painottamalla, että tietoturvallisuudesta keskustellaan koko kohdeyrityksen laajuisesti liiketoiminnan näkökulmasta. Lisäksi vastauksiin pyydettiin usein perusteluja ja tarkennuksia, jotka auttoivat tutkijaa arvioimaan oliko haastateltu ymmärtänyt asian oikein.

Tutkimuksen validiteettia heikentää vahvasti laadulliselle tutkimukselle ominainen subjektiivisuus. Tutkijan henkilökohtaisella näkemyksellä ja aihepiirin ymmärryksen määrällä oli suuri merkitys sekä haastattelujen tulkinnassa että mittariston suunnittelussa. Haastattelujen tulkinnasta keskusteltiin kohdeyrityksen edustajan kanssa, mikä osaltaan paransi tutkimuksen validiteettia. Kattavampi esitieto aihepiiristä olisi voinut auttaa myös muodostamaan paremmin tietoturvallisuuden tilaa kuvailevia asioita ja tietotarpeita esiintuovan haastattelun kuin tässä tutkimuksessa käytetty haastattelu. Vaikka käytettyjen menetelmien sopivuus tähän työhön on pyritty perustelemaan, ei voida olla täysin varmoja olisiko jollain muulla menetelmällä pystytty kuvailemaan tutkittavaa ilmiötä kattavammin tai yksityiskohtaisemmin. Varmasti voidaan ainakin sanoa, että tietoturvallisuuden mittaamista tulee tutkia lisää sekä tieteellisesti että kohdeyrityksen näkökulmasta. Näin voidaan mahdollisesti jälkikäteen nähdä, olivatko tässä tutkimuksessa käytetyt menetelmät hyviä ja riittävän tarkkoja vai pelkästään suuntaa-antavia.

Kirjallisuuslähteitä, jotka liittyvät suoraan tutkimuksen ydinteemaan ja näkökulmaan, ei ole merkittävästi saatavilla. Tämä johtuu kenties siitä, että tietoturvallisuus nähdään organisaation toiminnan tukifunktiona. Tästä syystä mittareita on kehitelty jonkin verran tietoturvapäällikön näkökulmasta, mutta ne eivät sovellu tietoturvapäällikön ja johdon väliseen kommunikointiin. Toinen syy on, että tietoturvallisuutta käsitellään usein teknisenä asiana, jolloin kirjallisuuslähteiden aihepiiri on tekninen. Yksi tutkimuksen haas-

teista muodostuikin tutkijan vastuusta soveltaa ja yhdistää edellä kuvatun aihepiirin tutkimusta korkeamman tason mittaamiseen sopiviksi. Tietoturvallisuuden merkityksen kasvaessa liiketoimintajohdon kiinnostus aiheeseen saattaa lisätä tutkimuksia, joissa pohditaan kokonaisvaltaisempaa esitystä tietoturvallisuuden mittaamisesta. Tämän tutkimuksen tuloksia voidaan yleistää käyttäväksi myös muissa yrityksissä kahdesta syystä. Ensinnäkin mittariston viitekehys rakennettiin tasapainotetun tuloskortin perusteella, joka on yleisesti tunnettu ja laajasti hyödynnetty menetelmä arvioida yrityksen tilaa laajasta näkökulmasta. Toisekseen mittaristo on helposti muunneltavissa sen mukaan, miten eri yritykset näkevät oman tietoturvallisuutensa. Suorittamalla tässä tutkimuksessa kuvaillut haastattelut voidaan yleisesti löytää organisaation tietotarpeet tietoturvallisuudesta, jotka voidaan liittää tutkimuksen tuloksena muodostettuun mittariston viitekehykseen.

Tutkimuksen teoriaosuutta voidaan kritisoida lähteiden käytöstä, sillä tietoturvallisuuden mittaamiseen liittyen lähteitä on vähän, kuten edellä mainittiin. Tästä syystä tutkimuksessa viitattiin usein standardeihin ja valtionhallinnon suosituksiin. Esimerkiksi mittareiden maturiteettiin liittyen ei löydetty tieteellisesti relevanttia lähdettä. On siis huomioitava, että jokin tärkeä näkökulma on saattanut jäädä huomioimatta. Tosin tutkimuksen tavoitteena oli luoda uutta tietoa vähän tutkitusta ja vaikeasti hahmotettavasta ilmiöstä, jolloin tutkijan ymmärrys ja esitieto tutkimuksen aihepiireistä oli tärkeää. Hyvä teoreettinen tai käytännönläheinen esitietämys tutkittavasta aiheesta on myös yleisesti toimintatutkimukseen liittyvä menestystekijä, joka lisää sen uskottavuutta (Gummesson 2000, s. 121). Tässä tutkimuksessa esitieto muodostettiin ja esitettiin teoriaosuuden kautta, mutta käytännönläheistä tietämystä ei tutkijalla aiheesta ennestään ollut. Lisäksi käytetyt tutkimusmenetelmät on esitelty ja niiden suhde toisiinsa on kuvattu tarkasti. Nämä voidaan nähdä tutkimuksen uskottavuutta lisäävinä tekijöinä.

Tutkimuksen teemahaastattelujen uskottavuutta vähentää se, että niihin osallistui vain kahdeksan henkilöä. Toisaalta haastatellut edustivat mittariston kohderyhmää ja heiltä saatua näkökulma siitä, miksi tietoturvallisuutta mitattaisiin ja mitkä ovat tärkeimpiä asioita sen suhteen. Koska näkökulma mittaamiseen oli yleisjohdollinen, tukee haastattelut tutkimustulosten laajennettavuutta myös muihin yrityksiin. On kuitenkin mainittava, että usein toimintatutkimuksen ongelmana saattaa olla, että tutkija kohdeyrityksen edustajat eivät täysin luota ulkopuoliseen tutkijaan, jolloin hänelle saatetaan jättää kertomatta olennaisia asioita (Levin et al. 2002). Tässä tutkimuksessa riski huonoon tiedonsaantiin teemahaastatteluissa ja siten epätäydellisiin tuloksiin on suuri, sillä tietoturvallisuus on aihepiirinä todella arka ja kohdeyritys suhtautui tutkimukseen aluksi epäilevästi. Riski toteutui konkreettisimmin siten, että kohdeyrityksen edustajat olivat haluttomia arvioimaan mittaristoa. Tutkimuksen uskottavuutta tukee kuitenkin se, että sekä kohdeyrityksen toimitusjohtaja että tietoturvapäällikkö hyväksyivät ja tukivat sen toteuttamista. Läheistä ja avointa suhdetta kohdeyrityksen kanssa, mikä on Iversenin et al. (2004) mukaan tärkeä menestystekijä toimintatutkimuksissa, ei kuitenkaan onnistuttu

muodostamaan. Kohdeyrityksen anonymiteetti säilytettiin sensuroimalla siihen viittaavat ja sen ominaispiirteitä kuvailevat asiat. Tämän ansioista tutkimuksessa tietoturvallisuuteen liittyviä asioita käsiteltiin yleistettävällä tavalla, mikä tukee sitä, että tämän tutkimuksen tuloksia voidaan hyödyntää myös muissa yrityksissä.

Tutkimuksen voidaan nähdä onnistuneen, sillä siinä käytettyjen menetelmien avulla pystyttiin muodostamaan kuvaus siitä, mitä kohdeyrityksen tietoturvallisuuden mittaaminen on liiketoiminnan näkökulmasta. Käytetyt menetelmät jo itsessään ovat keino ymmärtää tietoturvallisuuden tila ja muodostaa ehdotuksia siitä, miten sitä voidaan ohjata tietoturvastrategian mukaisesti. Varsinkin teemahaastattelujen ja aineiston sisällönanalyysin avulla löydettiin kohdeyrityksen tietoturvallisuuden menestystekijät. Toimintatutkimus kokonaisuudessaan oli mittariston kehitysprojekti, jonka lopputuloksena muodostui tietoturvamittaristo. Mittariston käyttöönottamalla on mahdollista ensinnäkin asettaa tavoitteita tietoturvallisuudelle ja toisaalta seurata, kuinka hyvin tavoitteet toteutetaan. Kaiken kaikkiaan tutkimusta ja saavutettuja tuloksia voidaan pitää hyvänä pohjatyönä myöhemmille tutkimuksille ja mittariston käyttöönotolle.

7.4 Jatkotutkimusaiheet

Tutkimuksessa keskityttiin ymmärtämään tietoturvallisuutta ja sen mittaamista. Tätä varten pyrittiin luomaan kuva siitä, mitä tietoturvallisuudella tarkoitetaan sekä esittelemään, miten mittaaminen tukee johtamista. Teoreettisen tarkastelun kannalta rajattiin pois jatkuvuudenhallinta ja siihen liittyvät suunnitelmat. Laajemmat tutkimukset siitä, kuinka hyvin jatkuvuussuunnitelmien ohessa voitaisiin tunnistaa mittareita tai kuinka hyvin mittaaminen tukisi organisaation toiminnan jatkuvuutta, voisivat olla tarpeen. Empiirisessä osuudessa lopputulokseksi muodostui tietoturvamittaristo, jonka käyttöönottoa ei tämän tutkimuksen puitteessa pystytty toteuttamaan. Käyttöönottoon liittyvien haasteiden ja mittausdatan keräämiseen liittyvien ratkaisujen tutkiminen vaativat jatkotutkimusta.

Mittariston käytettävyyden parantamiseen liittyen tulisi tunnistaa erilaisia visualisointikeinoja. Hyvin toteutetun visualisoinnin avulla mittareiden tuloksia voi ymmärtää ja vertailla tehokkaasti. Mittariston visualisoinnin suunnittelu ja käytännön toteutus muodostaakin oman tutkimusalueensa. Mittariston käyttöön oton lisäksi myös sen käyttöä olisi syytä tutkia. Käytön tutkimiseen soveltuu esimerkiksi pitkittäistutkimus, jonka aikana mittaristoa päivitettäisiin, arvioitaisiin ja ylläpidettäisiin luvussa 3.4 esitetyn kuvan mukaisesti. Mielenkiintoinen aihe olisi myös toistaa sama tutkimus kohdeyrityksessä vuoden tai kahden päästä ja nähdä, miten mittauksen kohteet ovat muuttuneet ja pystytäänkö yrityksessä käyttämään jo korkeamman maturiteettitason mittareita. Toisaalta jatkotutkimuksena voitaisiin syventyä yhden liiketoimintalinjan tietoturvallisuuteen ja tutkia keinoja mitata sen tietoturvallisuuden tilaa yksityiskohtaisemmin. Tämä vaatisi

laajempaa haastattelukierrosta useilta organisaatiotasoilta sekä laajaa ymmärrystä niiden liiketoimintaprosesseista.

Tutkimuksen aihekenttää, tietoturvallisuuden mittaamista ja tietoturvallisuuden tilan esittämistä johdolle, on tieteellisesti tutkittu melko vähän. Tutkimukset osoittavat mittareita usein tietoturvapäällikölle tai järjestelmien ylläpitäjille. Tästä syystä tätä tutkimusta tutkimuksille, joissa käsitellään tietoturvallisuuden tilan esittämistä holistisella tasolla, on tarvetta tulevaisuudessa. Näin saadaan vertailukelpoisia tuloksia useista eri yrityksistä eri toimialoilta ja liitetään myös teoreettisesta näkökulmasta tietoturvallisuutta osaksi liiketoimintaa.

LÄHTEET

Ariyachandra, T. & Frolick, M. 2008. Critical Success Factors in Business Performance Management – Striving for Success. Information Systems Management. Vol 25, no. 2, ss. 113-120.

Au, D. 2012. Getting the CISO a Seat. Security Week, Internet and Enterprise Security News, Insights & Analysis. [WWW]. [Viitattu: 25.7.2012] Saatavilla: http://www.securityweek.com/getting-ciso-seat

Awad, E. & Ghaziri, H. 2004. Knowledge Management. New Jersey, USA, Pearson Educaiton. 456 s.

Barabanov, R., Kowalski, S. & Yngström, L. 2011 Information Security Metrics. State of the Art. DSV Report series no. 11-007.

Baskerville, R. & Dhillon, G. 2008. Information Systems Security Strategy. A Process View. Straub, D., Goodman, S. & Baskerville, R. (toim.) Information Secure. Policy, Processes and Practises. Vol. 11, ss. 15-45.

Bourne, M., Mills, J., Wilcox, M., Neely, A. & Platts, K. 2000. Designing, implementing and updating performance measurement systems. International Journal of Operations & Production Management. Vol. 20, no. 7, ss. 754–771.

Brotby, W.K. 2009. Information Security Management Metrics. A Definitive Guide to Effective Security Monitoring and Measurement. CRC Press. 211 s.

Chapin, D. & Akridge, S. 2005. How Can Security Be Measured? Information Systems Control Journal. Vol. 2.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. & Robinson, W. 2007. Information Security. Performance Measurement Guide for Information Security (DRAFT). NIST Special Publication no. 800-55, Revision 1.

CIS, 2012. Community. [WWW]. [Viitattu: 25.l0.2012]. Saatavilla: http://benchmarks.cisecurity.org/en-us/?route=community

CIS, 2009. The CIS Security Metrics. Consensus Metric Definitions v1.0.0. Center for Internet Security (CIS)

Datta, S. & Banerjee, P. 2011. Guideline for Performance Measures of Information Security of IT Network and Systems. International Journal of Research and Reviews in Next Generation Networks. Vol. 1, No. 1. ss. 39-43.

Davenport, T. & Prusak, L. 1998. Working Knowledge: How Organizations Manage What They Know. Boston, USA, Harvard Business School Press. 199 s.

Davis, J. 2004. Security Patch Management. Tipton, H. & Krause, M. (toim.) Information Security Handbook. 5. painos. Boca Raton, CRC Press. ss. 689-696.

Demetz, L. & Bachlechner, D. 2012. To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool. 11th Annual Workshop on the Economics of Information Security.

Desouza, K. 2007. Managing Knowledge Security. Lontoo, Kogan Page. 200 s.

Dhillon, G. & Backhouse, J. 2000. Information system security management in the new millennium. Communications of the ACM. Vol. 43, no. 7, ss. 125-128.

Enisa. 2012. European Network and Information Security Agency.

Ghauri, P. & Grønhaug, K. 2005. Research Methods in Business Studies: A Practical Guide. 3. painos. Englanti, Pearson Education. 257 s.

Gummesson, E. 2000. Qualitative Methods in Management Research. 2. painos. Sage Publications,Thousand Oaks. 264 s.

Hannula, M., Korsman, U., Pajarre, E. & Seppänen, M. 2002. Ohejeita opinnäytetyön kirjoittajalle. Tuotantotalouden osaston diplomi-, seminaari- ja harjoitustyöohje. Tampere. 36 s.

Hare, C. 2004. Policy Development. Tipton, H. & Krause, M. (toim.) Information Security Handbook. 5. painos. Boca Raton, CRC Press. ss. 925-944

Heimerl, J. 2012a. Security is Not Just External – Don't Forget the "Other" Security. Security Week. Internet and Enterprise Security News, Insights & Analysis. [WWW]. [Viitattu: 2.10.2012]. Saatavilla: http://www.securityweek.com/security-not-just-external-dont-forget-other-security

Heimerl, J. 2012b. Best Practice: Can You Really Define ‘Best’ Security? Security Week. Internet and Enterprise Security News, Insights & Analysis. [WWW]. [Viitattu: 2.8.2012]. Saatavilla: http://www.securityweek.com/best-practice-can-you-really-define-best-security

Henning, R. 2001. Proceedings of Workshop on Information Security System, Scoring and Ranking – Information System Security Attribute Quantification or Ordering. ACSA and MITRE, USA.

Herrmann, D. 2007. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilance, and ROI. Boca Raton, Auerbach Publications. 848 s.

HTL. 22.4.1999/523. Henkilötietolaki.

ISO 2012. ISO Standards. [WWW]. [Viitattu: 6.8.2012] Saatavilla: http://www.iso.org/iso/home/standards.htm

ISO/IEC 27001:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS. 66 s.

ISO/IEC 27004. 2009. Information technology - Security techniques – Information Security - Information security management – Measurement. International Standard. 55 s.

Iversen, J., Mathiassen, L. & Nielsen, P. 2004. Managing Risk in Software Process Improvement: An Action Research Approach. MIS Quarterly. Vol. 28, no. 3, ss. 395-434.

Jansen, W. 2009. Directions in security metrics research. National Institute of Standards and Technology. U.S. Department of Commerce. 21 s.

Jaquith, A. 2007. Security Metrics. Replacing Fear, Uncertainty, and Doubt. USA, Addison-Wesley. 306 s.

Juneja, D., Arora, K. & Duggal, S. 2011. Developing Security Metrics for Information Security Measurement Systems. International Journal of Enterprise Computing and Business System ISSN (Online) : 2230-8849. Vol. 1, no. 2.

Kairab, S. 2005. A Practical Guide to Security Assesment. Boca Raton, CRC Press. 498 s.

Kaplan, R.S. & Norton, D.P. 2004. Strategiakartat. Aineettoman pääoman muuttaminen mitattaviksi tuloksiksi. Helsinki, Talentum. 404 s.

Kaplan, R.S. & Norton, D.P. 1992. The Balanced Scorecard – Measures That Drive Performance. Harvard Business Review. s. 71–79.

Kasanen, E., Lukka, K. & Siitonen, A. 1991. Konstruktiivinen tutkimusote liiketaloustieteessä. Liiketaloudellinen Aikakauskirja, Vol. 3, ss. 301–327.

Kaydos, W. 1999. Operational Performance Measurement: Increasing Total Productivity. Boca Raton, St. Lucie Press. 245 s.

Kayworth, T & Whitten, D. 2010. Effective Information Security Requires a Balance of Social and Techonology Factors. MIS Quarterly Executive, Vol. 9, no. 3, ss. 163-175.

Koskinen, I., Alasuutari, P. & Peltonen, T. 2005. Laadulliset menetelmät kauppatieteissä. Tampere, Vastapaino. 350 s.

Kowalski, S. & Barabanov, R. 2011. Modelling Static and Dynamic Aspects of Security: A Socio-Techincal View

Krutz, R. & Vines, R.D. 2004. The CISSP Prep Guide. Mastering the CISSP and ISSEP Exams. 2. painos. USA, Wiley Publishing Inc. 1024 s.

Kujansivu, P., Lönnqvist, A., Jääskeläinen, A. & Sillanpää, V. 2007. Liiketoiminnan aineettomat menestystekijät. Mittaa, kehitä ja johda. Helsinki, Talentum. 204 s.

Kwon, J. & Johnson, E. Security Resources, Capabilities and Cultural Values: Links to Security Performance and Compliance. Proceedings of Workshop on the Economics of Information Security, Berliini, Saksa, Kesäkuun 25-26, 2012.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Helsinki, WSOY. 307 s.

Landwehr, C. 2001. Computer Security. International Journal on Information Security, Vol. 1, No 1, ss. 3-13.

Lemos, R. 2012. Five Strategic Security Metrics To Watch. Tech Center: Security Monitoring. [WWW]. [Viitattu: 31.3.2012]. Saatavissa: http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232601457/five-strategic-security-metrics-to-watch.html

Levin, D., Cross, R., Abrams, L. & Lesser, E. 2002. Trust and Knowledge Sharing: A Critical Combination. IBM Institute for Knowledge-based Organizations.

Lippman, R., Riordan, J., Yu, T. & Watson, K. 2012. Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics. Massachusetts, Lincoln Laboratory. 108 s.

Lönnqvist, A. 2004. Measurement of Intangible Success Factors: Case Studies on the Design. Implementation and Use of Measures. Tampere, Tampere University of Technology, Publication. 475 s.

Lönnqvist, A. 2004. Measurement of Intangible Success Factors: Case Studies on the Desing, Implementation and Use of Measures. Tampere, Tampereen Teknillinen Yliopisto. 475 s.

Lönnqvist, A., Blomqvist, K., Hannula, M., Kianto, A., Kärkkäinen, H., Maula,M., & Ståhle, P. 2007. Tietojohtaminen tutkimusalueena. Tampere, Mediapinta. 141 s.

Lönnqvist, A., Kujansivu, P. & Antikainen, R. 2006. Suorituskyvyn mittaaminen - Tunnusluvut asiantuntijaorganisaation johtamisvälineenä. Helsinki, Edita Publishing Oy. 162 s.

Marr, B. & Schiuma, G. 2003. Business performance measurement – past, present, and future. Management Decisions. Vol. 41, no. 8. ss, 680-687.

Neely, A., Gregory, M. & Platts, K. 1995. Performance measurement system design: A literature review and research agenda. International Journal of Operations & Production Management. 2005. Vol. 25, no. 12. ss, 1228 – 1263.

Neely, A., Mills, J., Platts, K., Richards, H., Gregory, M., Bourne, M. & Kennerley, M. 2000. Performance Measurement System Design: Developing and Testing a Process-Based Approach. International Journal of Operations & Production Management. Vol. 20, no. 10, ss. 1119-1145.

Neilimo, K. & Uusi-Rauva, E. 1997. Johdon Laskentatoimi. Helsinki, Edita. 327.

Neilimo, K. & Näsi, J. 1980. Nomoteettinen tutkimusote ja suomalainen yrityksen taloustiede: Tutkimus postivismin soveltamisesta. Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja. Tampere, Tampereen yliopisto. 82 s.

Nonaka, I & Takeuchi, H. 1995. Knowledge Creating Company. How Japanese Companies Create the Dynamics of Innovation. New York, Oxford University Press. 284 s.

Olkkonen, T. 1994. Johdatus teollisuustalouden tutkimustyöhön. 2. painos. Espoo, Teknillinen korkeakoulu. Raportti 152. 143 s.

Otley, D. 1999. Performance management: a framework for management control systems research. Management Accounting Research. vol. 10. ss. 363-382.

Ozier , W. 2004. Risk Analysis and Assessment. Tipton, H. & Krause, M. (toim.) Information Security Handbook. 5. painos. Boca Raton, CRC Press. ss. 795-820.

Packova, V. & Karacsony, P. 2010. Designing and Implementing Performance Management Systems. Business Performance Measurement and Management. Vol. 6, ss. 241-249.

Paulk, M., Weber, S., Garcia, S., Chrissis M.B. & Bush, M. 1993. Capability maturity model, version 1.1. Software, IEEE. Vol. 10, no. 4, ss. 18-27.

Parmenter, D. 2006. The new thinking on key performance indicators. Finance & Management. Vol. 5, no. 133, ss. 1-4.

Pekkola, S. 2012. Patruunan ääntä etsimässä. Tietoviikko. [WWW]. [Viitattu: 3.10.2012]. Saatavilla: http://www.tietoviikko.fi/cio/blogit/ict_standard_forum/patruunan+aanta+etsimassa/a843475

Peltier, T., Peltier, J. & Blackley, J. 2004. Fundementals of Information Security. Boca Raron, CRC Press. 280 s.

Pettigrew, J. 2012. Decision-Making by Effective Information Security Managers. Väitöskirja, Arizona, University of Arizona. 346 s.

Pironti, J. 2007. Developing metrics for effective information security governance. Information Systems Control Journal. Vol. 2, ss. 33-38.

Pirttimäki, V. 2007. Conceptual analysis of business intelligence. South African Journal of Information Management. Vol. 9, no. 2.

Rashid, F. 2012. Smashing the Future: A Look Back, and the Future of Security. Security Week. Internet and Enterprise Security News, Insights & Analysis. [WWW]. [Viitattu: 31.7.2012]. Saatavilla: http://www.securityweek.com/smashing-future-look-back-and-future-security

Ryan, J. & Ryan, D. 2008. Performance Metrics for Information Security Risk Management. Security & Privacy, IEEE. Vol. 6, no. 5. ss. 38-44.

Saarela-Kinnunen, M. & Eskola, J. 2001. Tapaus ja tutkimus = Tapaustutkimus? Aaltola, J. & Valli, R. (toim.) Ikkunoita tutkimusmetodeihin – Metodin valinta ja aineiston keruu: Virikkeitä aloittelevalle tutkijalle. Jyväskylä, PS-Kustannus Oy, ss. 158-169.

Saari, S. 2006. Tuottavuus. Teoria ja mittaaminen liiketoiminnassa. Espoo, Mido Oy. 272 s.

Savola, R., Fruhwirht, C. & Pietikäinen, A. 2012. Risk-Driven Security Metrics in Agile Software Development – An Industrial Pilot Study. Journal of Universal Computer Science, Vol. 18, no. 12, ss. 1679-1702.

Savola, R. 2010. On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems. IJCSNS International Journal of Computer Science and Network Security, Vol. 10, no. 1, ss. 230-239.

Savola, R. 2007. Towards a taxonomy for information security metrics. Proceedings of the 2007 ACM workshop on Quality of protection, New York, USA, 2007. ss. 28-30

Shorten, B. 2004. Information Security Policies from the Ground Up. Tipton, H. & Krause, M. (toim.) Information Security Handbook. 5. painos. Boca Raton, CRC Press. ss. 917-924

Sink, D. 1983. Much Ado About Productivity: Where Do We Go From Here. Industrial Engineering. Vol. 15, no. 10, ss. 36-48.

Straub, D. Goodman, S. & Baskerville, R. 2008. Framing the Information Security Process in Modern Society. Straub, D. Goodman, S. Baskerville, R. (toim.) Information Secure. Policy, Processes and Practises. Vol. 11, ss. 5-12.

Susman, G. & Evered, R. 1978. An Assessment of the Scientific Merits of Action Research. Administrative Science Quarterly. Vol. 23, No. 4, ss. 582-603.

Swanson, M., Bartol, N., Sabato, J., Hash, J. & Graffo, L. 2003. Security Metrics Guide for Information Technology Systems. NIST Special Publication. no. 800-55.

Sydänmaanlakka, P. 2004. Älykäs organisaatio. Helsinki, Talentum Media Oy. 299 s.

Thierauf, R. 2001. Effective Business Intelligence Systems. USA, Quarum Books. 370 s.

Tipton, H. & Krause, M. 2004. Information security management handbook. 5. painos. CRC Press, Boca Raton. 2036 s.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. 4. painos. Helsinki, Tammi. 159 s.

VAHTI 3/2007. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaa. Valtionvarainministeriö.

VAHTI 2/2008. Tärkein tekijä on ihminen – henkilöturvallisuus osana tietoturvallisuutta. Valtionvarainministeriö.

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Valtionvarainministeriö.

VAHTI 2/2011. Johdon tietoturvaopas. Valtionvarainministeriö.

Valtionvarainministeri 2012. Julkisen hallinnon ICT. [WWW]. [Viitattu: 6.8.2012]. Saatavilla: http://www.vm.fi/vm/fi/16_ict_toiminta/index.jsp

Vaughn, R., Henning, R. & Siraj, A. 2003. Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy. Proceedings of 36th Hawaii International Conference on System Sciences HICSS 03. Washington, USA, IEEE Computer Society.

Whitman, M. 2008. Security Policy: From Desing to Maintanance. Straub, D. Goodman & S. Baskerville, R. (toim.) Information Secure. Policy, Processes and Practises. Vol. 11, ss. 123-151.

Whitman, M., Mattord, H. 2011. Principles of information security. 4. painos. USA, Course Technology. 617 s.

Wiander, T. 2007. Positive and Negative Findings of the ISOIEC 17799 Framwork. 18th Australasian Conference on Information Systems. ss. 615-621.

Wilson, T. 2012. End Users Still Don't Know How To Handle Personal Data, Study Finds. Dark Reading. [WWW]. [Viitattu: 31.7.2012]. Saatavilla: http://www.darkreading.com/identity-and-access-management/167901114/security/privacy/240003989/end-users-still-don-t-know-how-to-handle-personal-data-study-finds.html

Yin, R. K. 2003. Case Study Research: Desing and Methods. 3. painos. California, US Sage Publications. 181 s.

Ylisirniö, P. 2011. Strategian mittaaminen. Helsinki, WSOYpro OY. 227 s.

LIITE 1: TEEMAHAASTATTELUIDEN HAASTATTELURUNKO

Haastattelun tausta ja valmistelu

- Kuinka pitkään olet ollut yrityksessä?
- Asteikolla 1-5, kuinka hyvin tunnet yrityksen tietoturvallisuuden ja sen hallintakeinot?
- Vaikuttaako tietoturvallisuus henkilökohtaisella tasolla päätöksentekoon?
- Millaisissa tilanteissa hyödyntäisit tietoturvallisuuteen liittyviä mittareita?

Teemahaastattelurunko

Miksi mitataan: Tietoturvallisuuden mittaamistarpeen kartoitus

1. Millä arvosanalla 1-10 kuvailisit yrityksen tietoturvan tilaa?
    - Mitkä tekijät tähän vaikuttavat?
    - Millä perusteella?

2. Täyttääkö yritys sille asetetut tavoitteet tietoturvallisuuden näkökulmasta?
    - Mitkä nämä tavoitteet ovat?
    - Miten pystyt varmistamaan tämän?

3. Kuinka usein tietoturvallisuudesta raportoidaan?
    - Mitkä ovat mielestäsi tärkeimpiä asioita?
    - Entä vähiten tärkeimpiä?
    - Miten raportointia voitaisiin kehittää?

4. Mikä on subjektiivinen tavoite tietoturvallisuudelle seuraavan 12kk ajalle?
    - esim. Viisi tärkeintä asiaa

Mitä mitataan: Tietoturvan mittaamisen liittäminen liiketoimintaan ja muuhun mittaamiseen

5. Mitä mittareita seuraat päätöksenteon tukena?
    - Mitä lisätietoa kaipaat päätöksenteon tueksi tietoturvallisuuden näkökulmasta?

6. Mitkä ovat liiketoimintayksikön/yrityksen toiminnan kannalta tärkeimmät prosessit?

7. Mitkä ovat suurimmat uhat edellä mainittuihin?

8. Mitkä tietoturvallisuuteen liittyvät asiat vaikuttavat liiketoimintayksikön/yrityksen tuotantoon/prosesseihin?

9. Mitkä ovat liiketoimintayksikön/yrityksen tärkeimmät tietoturvamenetelmät?
    - Millä asioilla varmistetaan, että liiketoimintayksikön/yrityksessä toimitaan tietoturvallisesti?

10. Mitkä ovat liiketoimintayksikön keskeisimmät haasteet tietoturvallisuuden kannalta?
    - Miten näitä voidaan kuvailla?
    - Mistä nämä johtuvat?

11. Onko tietoturvallisuuden osuus eriytetty budjetissa?
    - Hyödynnätkö päätöksen teossa? TAI Kiinnostaako päätöksen teon kannalta?

Miten mitataan: Mittareiden suunnittelu

12. Minkälaisia tietoturvamittareiden tulisi olla?
    - Mitä mittarilukemien/indikaattoreiden pitäisi kertoa?
    - Miten mittariston voisi toteuttaa?

Lopuksi:

- Pitäisikö tietoturvallisuutta mielestäsi mitata?
    - Miksi?